

Enterprise Firewall with Application Awareness

- Enterprise Firewall , on page 1
- Overview of Enterprise Firewall, on page 1
- Restrictions, on page 3
- Configure Firewall Policies, on page 3
- Monitor Enterprise Firewall, on page 8
- Zone-Based Firewall Configuration Examples, on page 9

Enterprise Firewall

Table 1: Feature History

Feature Name	Release Information	Feature Description
Match Traffic Using Custom Applications	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Manager Release 20.14.1	Added support for matching traffic using a custom application in a custom-defined application list.

Cisco's Enterprise Firewall feature uses a flexible and easily understood zone-based model for traffic inspection, compared to the older interface-based model.

Overview of Enterprise Firewall

The Enterprise Firewall uses a flexible and easily understood zone-based model for traffic inspection, compared to the older interface-based model.

A firewall policy is a type of localized security policy that allows stateful inspection of TCP, UDP, and ICMP data traffic flows. Traffic flows that originate in a given zone are allowed to proceed to another zone based on the policy between the two zones. A zone is a grouping of one or more VPNs. Grouping VPNs into zones

allows you to establish security boundaries in your overlay network so that you can control all data traffic that passes between zones.

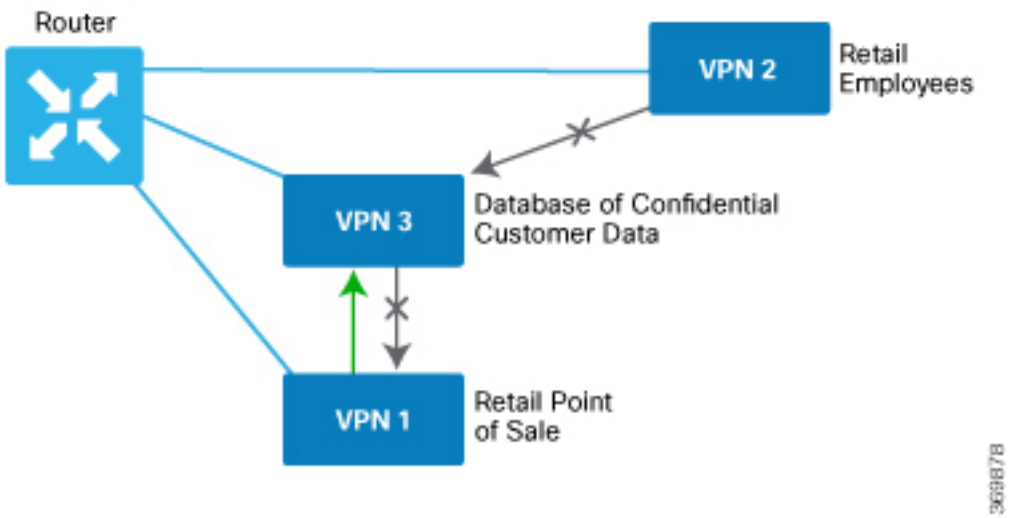
Zone configuration consists of the following components:

- Source zone—A grouping of VPNs where the data traffic flows originate. A VPN can be part of only one zone.
- Destination zone—A grouping of VPNs where the data traffic flows terminate. A VPN can be part of only one zone.
- Firewall policy—A security policy, similar to a localized security policy, that defines the conditions that the data traffic flow from the source zone must match to allow the flow to continue to the destination zone. Firewall policies can match IP prefixes, IP ports, the protocols TCP, UDP, and ICMP. Matching flows for prefixes, ports, and protocols can be accepted or dropped, and the packet headers can be logged. Nonmatching flows are dropped by default.
- Zone pair—A container that associates a source zone with a destination zone and that applies a firewall policy to the traffic that flows between the two zones.

Matching flows that are accepted can be processed in two different ways:

- Inspect—The packet's header can be inspected to determine its source address and port. When a session is inspected, you do not need to create a service-policy that matches the return traffic.
- Pass—Allow the packet to pass to the destination zone without inspecting the packet's header at all. When a flow is passed, no sessions are created. For such a flow, you must create a service-policy that will match and pass the return traffic.

The following figure shows a simple scenario in which three VPNs are configured on a router. One of the VPNs, VPN 3, has shared resources that you want to restrict access to. These resources could be printers or confidential customer data. For the remaining two VPNs in this scenario, only users in one of them, VPN 1, are allowed to access the resources in VPN 3, while users in VPN 2 are denied access to these resources. In this scenario, we want data traffic to flow from VPN 1 to VPN 3, but we do not want traffic to flow in the other direction, from VPN 3 to VPN 1.



The router provides Application Layer Gateway (ALG) FTP support with Network Address Translation – Direct Internet Access (NAT-DIA), Service NAT, and Enterprise Firewall. Service NAT support is added for FTP ALG on the client and not on the FTP Server.

Restrictions

- You can configure up to 500 firewall rules in each security policy in Cisco SD-WAN Manager.
- For packets coming from Overlay to Service side, the source VPN of the packet is defaulted to the destination VPN (service side VPN) for performing a Source Zone lookup when the actual source VPN cannot be determined locally on the branch. For example, a packet coming from VPN2 from the far end of a branch in a DC is routed through the Cisco Catalyst SD-WAN overlay network to VPN1 of a branch router. In this case, if the reverse route lookup for the source IP does not exist on the branch VPN1, the source VPN for that packet is defaulted to the destination VPN (VPN1). Therefore, VPN1 to VPN1 Zone-pair firewall policy is applied for that packet. This behavior is expected with policy-based routing configuration, and below are the examples of such a configuration.

Configuration	Command
Data policy: switching the VPN	`set-vpn`
Control policy and data policy: service chaining	`set service`

- Starting from Cisco IOS XE Catalyst SD-WAN Release 17.4.1a, you can configure geolocation and multiple list features in security policy on the edge devices. You can attach the security policy that has multiple list or geolocation feature enabled, only when the device is online with control connections up.
- The Application Layer Gateway (ALG) for L7 protocols causes traffic drop due to zone-based firewall inspection. If an application is running on a registered port which is assigned to another application, the traffic drops. For example, connection oriented syslog running on TCP port 514 which is assigned to another application drops. In such situations, disable application inspection or use a different port.
- Configuring service engine interfaces as a zone-member is not supported for releases prior to Cisco IOS XE Catalyst SD-WAN Release 17.7.1a. You must disable ZBFW or configure zone for VPN0 to VPN1 to allow the traffic.
- (Cisco Catalyst SD-WAN Manager Release 20.13.1 and earlier) When creating a security policy do not match traffic using a user-defined application list that includes a user-defined custom application.

  From Cisco Catalyst SD-WAN Manager Release 20.14.1, using a user-defined application list that includes a user-defined custom application is supported. However, the custom application cannot use IPv6 addresses in its match criteria.

Configure Firewall Policies

In Cisco SD-WAN Manager, you configure firewall policies from the **Configuration** > **Security** screen, using a policy configuration wizard. In the CLI, you configure these firewalls on the device.

Cisco SD-WAN Manager Firewall Configuration Procedure

To configure firewall policies, use the policy configuration wizard. The wizard is a UI policy builder that lets you configure the following policy components:

- Create rules – Create rules that you apply in the match condition of a firewall policy.

  Rules can consist of the following conditions:

  - Source data prefix(es) or source data prefix list(s).
  - Source port(s) or source port list(s).
  - Destination data prefix(es) or destination data prefix list(s).
  - Destination port(s) or destination port list(s).

Note Destination ports or destination port lists cannot be used with protocols or protocol lists.

  - Protocol(s) or protocol list(s).

- Define the order – Enter Edit mode and specify the priority of the conditions
- Apply zone-pairs – Define the source and destination zones for the firewall policy.

.

Note The following policy components are not supported on Cisco vEdge devices.

- Source port list(s)
- Destination port list(s)
- Protocol list
- FDQN list
- Geolocation list
- Application list
- Rule sets

Start the Security Policy Configuration Wizard

To start the policy configuration wizard:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Security**.
2. Click **Add Security Policy**.
3. Choose a security policy use-case scenario from one of the following:

- Compliance.
- Guest Access.
- Direct Cloud Access.
- Direct Internet Access.
- Custom.

4. Click **Proceed**.
5. Click **Create Add Firewall Policy**.
6. Click **Create New**.

   The Add Firewall Policy wizard is displayed.

Create Rules

1. Start the Security Policy Configuration Wizard
2. In the **Name** field, enter a name for the policy.
3. In the **Description** field, enter a description for the policy.
4. Depending on your release of Cisco SD-WAN Manager, do one of the following:
   - Cisco vManage Release 20.4.1 and later releases:
     a. Click **Add Rule/Rule Set Rule**.
     b. Click **Add Rule**.
   - Cisco vManage Release 20.3.2 and earlier releases: click **Add Rule**.

   The zone-based firewall configuration wizard opens.
5. Choose the order for the rule.
6. Enter a name for the rule.
7. Choose an action for the rule:
   - **Inspect**
   - **Pass**
   - **Drop**
8. If you want matches for this rule to be logged, check the **Log** check box.
9. Configure one or more of the following fields.



Note For the following fields, you can also enter defined lists or define a list from within the window.

Table 2: Firewall Rules

Field	Description
Source Data Prefixes	IPv4 prefixes or IPv6 prefixes or prefix lists.
Source Port(s)	Source port(s) and/or lists
Destination Data Prefix(es)	IPv4 prefixes or prefix list(s)
Destination Ports	Destination ports and/or lists **Note** Destination ports or destination port lists cannot be used with protocols or protocol lists.
Protocol(s)	Protocols and/or list(s)

10. Click **Save** to save the rule.
11. (Optional) Repeat steps 4–10 to add more rules.
12. Click **Save Firewall Policy**.

Apply Policy to a Zone Pair

Table 3: Feature History

Feature Name	Release Information	Description
Self Zone Policy for Zone-Based Firewalls	Cisco SD-WAN Release 20.3.1 Cisco vManage Release 20.3.1	This feature allows you to define firewall policies for incoming and outgoing traffic between a self zone of an edge router and another zone. When a self zone is configured with another zone, the traffic in this zone pair is filtered as per the applied firewall policy.

Note For IPSEC overlay tunnels in Cisco Catalyst SD-WAN, if a self zone is chosen as a zone pair, firewall sessions are created for SD-WAN overlay BFD packets if inspect action is configured for UDP.

However, for GRE overlay tunnels, if you chose a self zone as a zone pair with the inspect action of protocol 47, firewall sessions are created only for TCP, UDP, ICMP packets; but not BFD packets.

Warning Control connections may be impacted when you configure drop action from self-zone to VPN0 and vice versa. This applies for DTLS/TLS, BFD packets, and IPsec overlay tunnel.

Note On a Cisco vEdge device, packets to and from the management interface under VPN 512 do not go through the firewall module.

To apply policy to a zone pair:

1. Create security policy using Cisco SD-WAN Manager. For information see, Start the Security Policy Configuration Wizard.
2. Click **Apply Zone-Pairs**.
3. In the **Source Zone** field, choose the zone that is the source of the data packets.
4. In the **Destination Zone** field, choose the zone that is the destination of the data packets.

Note You can choose self zone for either a source zone or a destination zone, not both.

5. Click the plus (+) icon to create a zone pair.
6. Click **Save**.
7. At the bottom of the page, click **Save Firewall Policy** to save the policy.
8. To edit or delete a firewall policy, click the **...**, and choose the desired option.
9. Click **Next** to configure the next security block in the wizard. If you do want to configure other security features in this policy, click **Next** until the Policy Summary page is displayed.

Note When you upgrade to Cisco SD-WAN Release 20.3.3 and later releases from any previous release, traffic to and from a service VPN IPSEC interface is considered to be in the service VPN ZBFW zone and not a VPN0 zone. This could result in the traffic getting blackholed, if you allow traffic flow only between service VPN and VPN0 and not the intra service VPN.

You have to make changes to your ZBFW rules to accommodate this new behavior, so that the traffic flow in your system is not impacted. To do this, you have to modify your intra area zone pair to allow the required traffic. For instance, if you have a policy which has the same source and destination zones, you have to ensure the zone-policy allows the required traffic.

Create Policy Summary

1. Enter a name for the security policy. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.
2. Enter a description for the security policy. This field is mandatory.
3. Click **Save Policy** to save the security policy.

Apply a Security Policy to a Device

To apply a security policy to a device:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Device Templates** is called **Device**.

3. From the **Create Template** drop-down list, choose **From Feature Template**.
4. From the **Device Model** drop-down list, choose one of the devices.
5. Click **Additional Templates**.

   The **Additional Templates** section is displayed.
6. From the **Security Policy** drop-down list, choose the name of the policy you configured previously.
7. Click **Create** to apply the security policy to a device.
8. Click **…** next to the device template that you created.
9. Click **Attach Devices**.
10. Choose the devices to which you want to attach the device template.
11. Click **Attach**.

Monitor Enterprise Firewall

You can monitor Enterprise Firewall by using the statistics created for the firewall.

To monitor Enterprise Firewall and view statistics:

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose the **Monitor** > **Network**.
2. Choose a device from the list of devices.
3. Click **Real Time** in the left pane. A pop-up window appears with **Device Options**.
4. Click **Search**, and choose **Policy Zone Based Firewall Statistics** from the list to view the statistics for the firewall policies.

Note Firewall Charts and Policy statistics are not currently supported for Cisco vEdge devices from **Network** > **Firewall** dashboard. However, detailed statistics are available when you navigate from the Cisco SD-WAN Manager menu **Network** > **Real Time**.

Zone-Based Firewall Configuration Examples

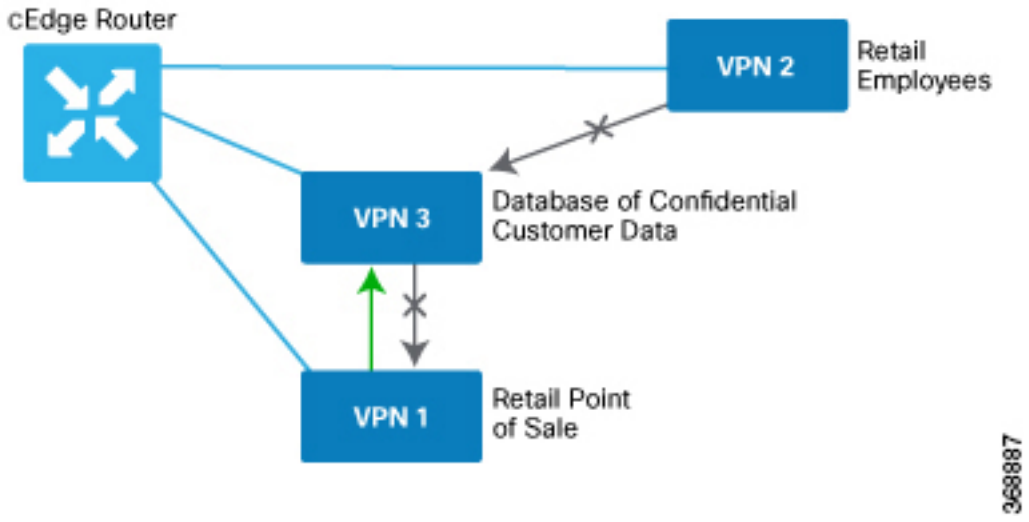
This topic provides an example of configuring a simple zone-based firewall using the CLI template or Cisco SD-WAN Manager.

Isolating Two VPNs

In this zone-based firewall configuration example, we have a scenario where a router is connected to three service-side networks:

- Guest network that provides point-of-sale (PoS) services
- Employee network
- Network that provides shared services, including shared printers and the customer database

We want users in the employee and guest networks to be able to access the shared services, but we do not want any traffic to be exchanged between the employee and guest networks. Similarly, we do not want any traffic that originates in the shared services network to enter into either the employee network or the guest network. The following figure illustrates this scenario:



In this figure:

- VPN 1 is the guest network used for PoS services.
- VPN 2 is the network used by the enterprise's employees.
- VPN 3 contains the shared services, including printers and customer databases.

The configuration consists of three sections:

- Define the zones.
- Define the zone-based firewall policy.
- Apply the zone-based firewall policy to a source zone and destination zone pair.

CLI Configuration

First, we define the zones for this scenario:

```
vEdge(config)# policy
vEdge(config-policy)# zone pos-zone vpn 1
vEdge(config-policy)# zone employee-zone vpn 2
vEdge(config-policy)# zone services-zone vpn 3
```

In this simple example, each zone corresponds to a single VPN. If you were to later add a second VPN for a discrete group of employees (let's say this is VPN 20) and you wanted this VPN to be subject to the same firewall policy, you could simply add this VPN to the employee zone:

```
vEdge(config-policy)# zone employee-zone vpn 20
vEdge(config-policy)# show full-configuration
policy zone employee-zone
  vpn 2
  vpn 20
 !
!
```

Next, we configure the zone-based firewall policy. The policy matches all traffic that is destined for VPN 3, which is the services zone, and which has an IP prefix of 10.2.2.0/24. Because we want the policy to allow traffic to flow from VPN 1 and VPN 2 to VPN 3, but we do not want traffic to flow in the reverse direction, we set the action to **pass**.

```
vEdge(config-policy)# zone-based-policy vpn-isolation-policy(config-zone-based-policy)#
sequence 10(config-sequence)# match destination-ip 10.2.2.0/24
vEdge(config-sequence)# action pass
```

We want to drop any traffic that does not match the zone-based filrewall policy:

```
vEdge(config-zone-based-policy)# default-action drop
```

In the final step of the configuration process, we apply the zone-based firewall policy to the zones. Here is the zone pairing between the guest and PoS zone and the services zone:

```
vEdge(config-policy)# zone-pair pos-services-pairing
vEdge(config-zone-pair)# source-zone pos-zone
vEdge(config-zone-pair)# destination-zone services-zone
vEdge(config-zone-pair)# zone-policy vpn-isolation-policy
```

And here is the pairing between the employee zone and the services zone:

```
vEdge(config-policy)# zone-pair employee-services-pairing
vEdge(config-zone-pair)# source-zone employee-zone
vEdge(config-zone-pair)# destination-zone services-zone
vEdge(config-zone-pair)# zone-pair employee-services-pairing
```

Here is a view of the entire policy:

```
vEdge(config-policy)# show full-configuration
 policy
 zone employee-zone
  vpn 2
! zone pos-zone
  vpn 1
 ! zone services-zone
  vpn 3
!
zone-pair employee-services-pairing
  source-zone      employee-zone
  destination-zone services-zone
```

```
  zone-policy      vpn-isolation-policy
 !
zone-pair services-pairing
  source-zone      pos-zone
  destination-zone services-zone
  zone-policy      vpn-isolation-policy
 !
zone-based-policy vpn-isolation-policy
  sequence 10
   match
   destination-ip 10.2.2.0/24
  !
   action pass
  !
!
 default-action drop
!
!
```

Verify Zone-based Firewall Statistics

Use the following CLI commands to verify the result of zone-based firewall statistics:

View Zone-based Firewall Sessions

The following is a sample output from the **show sdwan zonebfwdp sessions** command:

```
Device#show sdwan zonebfwdp sessions

        SRC  DST                                                                                  TOTAL      TOTAL
                  UTD
SESSION                                                                 SRC    DST                  SRC
  DST  VPN  VPN                                                    NAT    INTERNAL  INITIATOR  RESPONDER
  APPLICATION  POLICY
ID       STATE  SRC IP               DST IP                PORT   PORT  PROTOCOL       VRF
  VRF  ID   ID   ZP NAME              CLASSMAP NAME    FLAGS  FLAGS     BYTES      BYTES
     TYPE         NAME
-------------------------------------------------------------------------------------------------------------------------
13       open   2001:DB8::1        2001:DB8::1  53247       80    PROTO_L7_HTTP  1       1
    1    1    ZP_zone1_zone1_seq_1  seq_1-seq-1-cm_  -      0         96         298990
              -
```

View Zone-Pair Statistics

The following is a sample output from the **show sdwan zbfw zonepair-statistics** command:

```
Device#show sdwan zbfw zonepair-statistics
zbfw zonepair-statistics ZP_zone1_zone1_seq_1
 src-zone-name zone1
 dst-zone-name zone1
 policy-name   seq_1
 fw-traffic-class-entry seq_1-seq-1-cm_
  zonepair-name                 ZP_zone1_zone1_seq_1
  class-action                  Inspect
  pkts-counter                  7236
  bytes-counter                 4573618
  attempted-conn                9
  current-active-conn           0
  max-active-conn               1
  current-halfopen-conn         0
  max-halfopen-conn             1
  current-terminating-conn      0
```

```
 max-terminating-conn           0
 time-since-last-session-create 4373
 fw-tc-match-entry seq_1-seq-rule1-v6-acl_ 3
  match-type "access-group name"
 fw-tc-proto-entry 1
  protocol-name tcp
  byte-counters 4545768
  pkt-counters  7037
 fw-tc-proto-entry 4
  protocol-name icmp
  byte-counters 27850
  pkt-counters  199
 l7-policy-name                 NONE
fw-traffic-class-entry seq_1-seq-11-cm_
 zonepair-name                  ZP_zone1_zone1_seq_1
 class-action                   Inspect
 pkts-counter                   4947
 bytes-counter                  3184224
 attempted-conn                 5
 current-active-conn            0
 max-active-conn                1
 current-halfopen-conn          0
 max-halfopen-conn              0
 current-terminating-conn       0
 max-terminating-conn           0
 time-since-last-session-create 4480
 fw-tc-match-entry seq_1-seq-Rule_3-acl_ 3
  match-type "access-group name"
 fw-tc-proto-entry 1
  protocol-name tcp
  byte-counters 3184224
  pkt-counters  4947
 l7-policy-name                 NONE
fw-traffic-class-entry class-default
 zonepair-name                  ZP_zone1_zone1_seq_1
 class-action                   "Inspect Drop"
 pkts-counter                   11
 bytes-counter                  938
 attempted-conn                 0
 current-active-conn            0
 max-active-conn                0
 current-halfopen-conn          0
 max-halfopen-conn              0
 current-terminating-conn       0
 max-terminating-conn           0
 time-since-last-session-create 0
 l7-policy-name                 NONE
```

View Zone-Pair Drop Statistics

The following is a sample output from the **show sdwan zbfw drop-statistics** command:

```
Device#show sdwan zbfw drop-statistics
zbfw drop-statistics catch-all                 0
zbfw drop-statistics l4-max-halfsession        0
zbfw drop-statistics l4-too-many-pkts          0
zbfw drop-statistics l4-session-limit          0
zbfw drop-statistics l4-invalid-hdr            0
zbfw drop-statistics l4-internal-err-undefined-dir 0
zbfw drop-statistics l4-scb-close              0
zbfw drop-statistics l4-tcp-invalid-ack-flag   0
zbfw drop-statistics l4-tcp-invalid-ack-num    0
zbfw drop-statistics l4-tcp-invalid-tcp-initiator 0
zbfw drop-statistics l4-tcp-syn-with-data      0
```

```
zbfw drop-statistics l4-tcp-invalid-win-scale-option 0
zbfw drop-statistics l4-tcp-invalid-seg-synsent-state 0
zbfw drop-statistics l4-tcp-invalid-seg-synrcvd-state 0
zbfw drop-statistics l4-tcp-invalid-seg-pkt-too-old 0
zbfw drop-statistics l4-tcp-invalid-seg-pkt-win-overflow 0
zbfw drop-statistics l4-tcp-invalid-seg-pyld-after-fin-send 0
zbfw drop-statistics l4-tcp-invalid-flags      0
zbfw drop-statistics l4-tcp-invalid-seq        0
zbfw drop-statistics l4-tcp-retrans-invalid-flags 0
zbfw drop-statistics l4-tcp-l7-ooo-seg         0
zbfw drop-statistics l4-tcp-syn-flood-drop     0
zbfw drop-statistics l4-tcp-internal-err-synflood-alloc-hostdb-fail 0
zbfw drop-statistics l4-tcp-synflood-blackout-drop 0
zbfw drop-statistics l4-tcp-unexpect-tcp-payload 0
zbfw drop-statistics l4-tcp-syn-in-win         0
zbfw drop-statistics l4-tcp-rst-in-win         0
zbfw drop-statistics l4-tcp-stray-seg          0
zbfw drop-statistics l4-tcp-rst-to-resp        0
zbfw drop-statistics insp-pam-lookup-fail      0
zbfw drop-statistics insp-internal-err-get-stat-blk-fail 0
zbfw drop-statistics insp-dstaddr-lookup-fail  0
zbfw drop-statistics insp-policy-not-present   0
zbfw drop-statistics insp-sess-miss-policy-not-present 0
zbfw drop-statistics insp-classification-fail  0
zbfw drop-statistics insp-class-action-drop    0
zbfw drop-statistics insp-policy-misconfigure  0
zbfw drop-statistics l4-icmp-too-many-err-pkts 0
zbfw drop-statistics l4-icmp-internal-err-no-nat 0
zbfw drop-statistics l4-icmp-internal-err-alloc-fail 0
zbfw drop-statistics l4-icmp-internal-err-get-stat-blk-fail 0
zbfw drop-statistics l4-icmp-internal-err-dir-not-identified 0
zbfw drop-statistics l4-icmp-scb-close         0
zbfw drop-statistics l4-icmp-pkt-no-ip-hdr     0
zbfw drop-statistics l4-icmp-pkt-too-short     0
zbfw drop-statistics l4-icmp-err-no-ip-no-icmp 0
zbfw drop-statistics l4-icmp-err-pkts-burst    0
zbfw drop-statistics l4-icmp-err-multiple-unreach 0
zbfw drop-statistics l4-icmp-err-l4-invalid-seq 0
zbfw drop-statistics l4-icmp-err-l4-invalid-ack 0
zbfw drop-statistics l4-icmp-err-policy-not-present 0
zbfw drop-statistics l4-icmp-err-classification-fail 0
zbfw drop-statistics syncookie-max-dst         0
zbfw drop-statistics syncookie-internal-err-alloc-fail 0
zbfw drop-statistics syncookie-trigger         0
zbfw drop-statistics policy-fragment-drop      0
zbfw drop-statistics policy-action-drop        11
zbfw drop-statistics policy-icmp-action-drop   0
zbfw drop-statistics l7-type-drop              0
zbfw drop-statistics l7-no-seg                 0
zbfw drop-statistics l7-no-frag                0
zbfw drop-statistics l7-unknown-proto          0
zbfw drop-statistics l7-alg-ret-drop           0
zbfw drop-statistics l7-promote-fail-no-zone-pair 0
zbfw drop-statistics l7-promote-fail-no-policy 0
zbfw drop-statistics no-session                0
zbfw drop-statistics no-new-session            0
zbfw drop-statistics not-initiator             0
zbfw drop-statistics invalid-zone              18
zbfw drop-statistics ha-ar-standby             0
zbfw drop-statistics no-forwarding-zone        0
zbfw drop-statistics backpressure              0
zbfw drop-statistics zone-mismatch             0
zbfw drop-statistics fdb-err                   0
zbfw drop-statistics lisp-header-restore-fail  0
```

```
zbfw drop-statistics lisp-inner-pkt-insane     0
zbfw drop-statistics lisp-inner-ipv4-insane    0
zbfw drop-statistics lisp-inner-ipv6-insane    0
zbfw drop-statistics policy-avc-action-drop    0
zbfw drop-statistics l4-icmp-invalid-seq       0
zbfw drop-statistics l4-udp-max-halfsession    0
zbfw drop-statistics l4-icmp-max-halfsession   0
zbfw drop-statistics no-zone-pair-present      0
```

View Drop Statistics for Interfaces

The following is a sample output from the **show platform hardware qfp active statistic drop** command:

```
Device#show platform hardware qfp active statistic drop
Last clearing of QFP drops statistics : never

-------------------------------------------------------------------------
Global Drop Stats                          Packets                 Octets
-------------------------------------------------------------------------
Disabled                                      3963                 439403
FirewallInvalidZone                             18                   1170
FirewallPolicy                                  11                    938
IpTtlExceeded                                   12                   1050
Ipv4NoAdj                                      151                   8456
Ipv4NoRoute                                    326                  46997
Ipv6EgressIntfEnforce                         4212                 897007
Ipv6NoAdj                                        6                    456
Ipv6NoRoute                                      3                    168
Nat64v6tov4                                      6                    480
SdwanImplicitAclDrop                          7033                 408502
UnconfiguredIpv6Fia                           1349                 147590
```

View Drop Counts

The following is a sample output from the **show platform hardware qfp active feature firewall drop all** command:

```
Device#show platform hardware qfp active feature firewall drop all
-----------------------------------------------------------------------------
Drop Reason                                                          Packets
-----------------------------------------------------------------------------
Invalid L4 header                                                          0
Invalid ACK flag                                                           0
Invalid ACK number                                                         0
Invalid TCP initiator                                                      0
SYN with data                                                              0
Invalid window scale option                                                0
Invalid Segment in SYNSENT                                                 0
Invalid Segment in SYNRCVD                                                 0
TCP out of window                                                          0
TCP window overflow                                                        0
TCP extra payload after FIN                                                0
Invalid TCP flags                                                          0
Invalid sequence number                                                    0
Retrans with invalid flags                                                 0
TCP out-of-order segment                                                   0
SYN flood drop                                                             0
INT ERR:synflood h-tdl alloc fail                                          0
Synflood blackout drop                                                     0
TCP - Half-open session limit exceed                                       0
Too many packet per flow                                                   0
ICMP ERR PKT per flow exceeds                                              0
```

```
Unexpect TCP pyld in handshake                                    0
INT ERR:Undefined direction                                       0
SYN inside current window                                         0
RST inside current window                                         0
Stray Segment                                                     0
RST sent to responder                                             0
ICMP INT ERR:Missing NAT info                                     0
ICMP INT ERR:Fail to get ErrPkt                                   0
ICMP INT ERR:Fail to get Statbk                                   0
ICMP INT ERR:direction undefined                                  0
ICMP PKT rcvd in SCB close st                                     0
Missed IP hdr in ICMP packet                                      0
ICMP ERR PKT:no IP or ICMP                                        0
ICMP ERR Pkt:exceed burst lmt                                     0
ICMP Unreach pkt exceeds lmt                                      0
ICMP Error Pkt invalid sequence                                   0
ICMP Error Pkt invalid ACK                                        0
ICMP Error Pkt too short                                          0
Exceed session limit                                              0
Packet rcvd in SCB close state                                    0
Pkt rcvd after CX req teardown                                    0
CXSC not running                                                  0
Zone-pair without policy                                          0
Same zone without Policy                                          0
ICMP ERR:Policy not present                                       0
Classification Failed                                             0
Policy drop:non tcp/udp/icmp                                      0
PAM lookup action drop                                            0
ICMP Error Packet TCAM missed                                     0
Security policy misconfigure                                      0
INT ERR:Get stat blk failed                                       0
IPv6 dest addr lookup failed                                      0
SYN cookie max dst reached                                        0
INT ERR:syncook d-tbl alloc failed                                0
SYN cookie being triggered                                        0
Fragment drop                                                     0
Policy drop:classify result                                      11
ICMP policy drop:classify result                                  0
L7 segmented packet not allow                                     0
L7 fragmented packet not allow                                    0
L7 unknown proto type                                             0
L7 inspection returns drop                                        0
Promote fail due to no zone pair                                  0
Promote fail due to no policy                                     0
Firewall Create Session fail                                      0
Firewall No new session allow                                     0
Not a session initiator                                           0
Firewall invalid zone                                            18
Firewall AR standby                                               0
Firewall no forwarding allow                                      0
Firewall back pressure                                            0
Firewall LISP hdr restore fail                                    0
Firewall LISP inner pkt insane                                    0
Firewall LISP inner ipv4 insane                                   0
Firewall LISP inner ipv6 insane                                   0
Firewall zone check failed                                        0
Could not register flow with FBD                                  0
Invalid drop event                                                0
Invalid drop event                                                0
Invalid drop event                                                0
Invalid ICMP sequence number                                      0
UDP - Half-open session limit exceed                              0
ICMP - Half-open session limit exceed                             0
AVC Policy drop:classify result                                   0
```

```
Could not aquire session lock                                          0
No Zone-pair found                                                     0
```

For more information about the CLI commands, see Cisco IOS XE SD-WAN Qualified Command Reference.