Zone Based Firewall Commands

- alert (zone-based policy), on page 1
- app-visibility, on page 2
- class-map, on page 3
- class-map type inspect, on page 4
- class (policy-map), on page 5
- drop, on page 6
- flow-visibility, on page 7
- implicit-acl-logging, on page 8
- inspect, on page 8
- log (parameter-map type), on page 9
- log flow-export, on page 9
- log-frequency, on page 10
- match access-group, on page 11
- multi-tenancy, on page 11
- parameter-map type inspect-global, on page 12
- policy, on page 13
- policy-map type inspect, on page 15
- service-policy (zones), on page 16
- service-policy type inspect, on page 16
- vpn zone security, on page 17
- vpn (zone), on page 18
- zone pair security, on page 18
- zone security, on page 19

alert (zone-based policy)

To turn on or off console display of Cisco IOS stateful packet inspection alert messages, use the **alert** command in parameter-map type inspect configuration mode. To change the configured setting or revert to the default setting, use the **no** form of this command.

alert on
no alert

Syntax Description

on	Enables message logging for instant messenger application policy events.

Command Default

Alert messages are not issued.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE alert (zone-based policy) command.

Examples

```
Router(config)# parameter-map type inspect insp-params
Router(config-profile)# alert on
```

```
Router(config)# parameter-map type inspect-global
Router(config-profile)# alert on
```

app-visibility

To enable application visibility so that a router can monitor and track the applications running on the LAN use the **app-visibility** command. Use the **no** form of this command to disable application visibility.

app-visibility

Command Default

Disabled.

Command Modes

Policy configuration (config-policy)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

To enable NBAR feature to recognize applications. Use the **show sdwan app-fwd dpi** command to see DPI flows.

Examples

Enable application-visibility on a router:

```
Router(config)# policy
Router(config-policy)# app-visibility
```

class-map

To create a class map to be used for matching packets to a specified class and to enter QoS class-map configuration mode, use the **class-map** command in global configuration mode. To remove an existing class map from a device, use the **no** form of this command.

class-map { [**type inspect match-all**] | [**match-any**] } *class-map-name*
no class-map { [**type inspect match-all**] | [**match-any**] }

Syntax Description

type inspect	(Optional) Specifies the class-map type as inspect.
match-all	(Optional) Determines how packets are evaluated when multiple match criteria exist. Matches statements under this class map based on the logical AND function. A packet must match all statements to be accepted. If you do not specify the **match-all** or **match-any** keyword, the default keyword used is **match-all**.
match-any	(Optional) Determines how packets are evaluated when multiple match criteria exist. Matches statements under this class map based on the logical OR function. A packet must match any of the match statements to be accepted. If you do not specify the **match-any** or **match-all** keyword, the default keyword is used **match-all**.
class-map-name	Name of the class for the class map. The class name is used for both the class map and to configure a policy for the class in the policy map. **Note** You can enter the value for the *class-map-name* argument within quotation marks. The software does not accept spaces in a class map name entered without quotation marks.

Command Default

A class map is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `class-map` command.

Examples

```
class-map match-any BestEffort
  match qos-group 3
 !
 class-map match-any Bulk
  match qos-group 4
 !
 class-map match-any Critical
  match qos-group 1
 !
 class-map match-any Critical-Low
```

```
 match qos-group 2
!
class-map match-any BULK
 match qos-group 2
!
class-map match-any CONTROL-SIGNALING
 match qos-group 4
!
class-map match-any CRITICAL-DATA
 match qos-group 1
!
class-map match-any Default
 match qos-group 5
!
class-map match-any INTERACTIVE-VIDEO
 match qos-group 3
!
class-map match-any LLQ
 match qos-group 0
!
class-map match-any Queue0
 match qos-group 0
!
class-map match-any Queue1
 match qos-group 1
!
class-map match-any Queue2
 match qos-group 2
!
class-map match-any Queue3
 match qos-group 3
!
class-map match-any Queue4
 match qos-group 4
!
class-map match-any Queue5
 match qos-group 5
!
class-map type inspect match-all cmap
 match access-group name cmap
!
class-map match-any Queue4
 match qos-group 0
!
```

The following example configures the match criterion for a class map on the basis of a specified protocol for zone based policy firewall:

```
class-map match-any aa1-cm0_
match protocol test
match protocol mpeg2-ts
!
```

class-map type inspect

To create a Layer 3 and Layer 4 or a Layer 7 (application-specific) inspect type class map, use the **class-map type inspect** command in global configuration mode. To remove a class map from the router configuration file, use the **no** form of this command.

Layer 3 and Layer 4 (Top Level) Class Map Syntax
class-map type inspect {**match-any** | **match-all**} *class-map-name*
no class-map type inspect {**match-any** | **match-all**} *class-map-name*

Layer 7 (Application-Specific) Class Map Syntax
class-map type inspect { **match-any** | **match-all** } *class-map-name*
no class-map type inspect { **match-any** | **match-all** } *class-map-name*

Syntax Description

match-any	Determines how packets are evaluated when multiple match criteria exist. Packets must meet one of the match criteria to be considered a member of the class.
match-all	Determines how packets are evaluated when multiple match criteria exist. Packets must meet all of the match criteria to be considered a member of the class. **Note** The **match-all** keyword is available only with Layer 3, Layer 4, and SMTP type class maps.
class-map-name	Name of the class map. The name can have a maximum of 40 alphanumeric characters. The class map name is used to configure the policy for the class in the policy map.

Command Default

The behavior of the **match-any** keyword is the default.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE class-map type inspect command.

Examples

```
class-map type inspect match-any test-sRule_2-14-cm_
match protocol tcp
match protocol udp
!
class-map type inspect match-all test-seq-1-cm_
match access-group name test-seq-Rule_1-acl_
!
class-map type inspect match-all test-seq-11-cm_
match class-map test-sRule_2-14-cm_
!
```

class (policy-map)

To specify the name of the class whose policy you want to create or change or to specify the default class (commonly known as the class-default class) before you configure its policy, use the **class**command in policy-map configuration mode. To remove a class from the policy map, use the **no** form of this command.

class { *class-name* | **class-default** }

no class { *class-name* | **class-default** }

Syntax Description

class-name	Name of the class to be configured or whose policy is to be modified. The class name is used for both the class map and to configure a policy for the class in the policy map.
class-default	Specifies the default class so that you can configure or modify its policy.

Command Default

No class is specified.

Command Modes

Policy-map configuration (config-pmap)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `class (policy-map)` command.

Examples

The following example shows how to create two policy maps called “PMap” and "generic-cos" and configure two class policies in each policy map.

```
policy-map PMap
 class PMap-super-fast
  priority level 1
  police percent 5
 !
 class PMap-fast
  priority level 2
  police percent 5
 !
!
policy-map generic-cos
 class cos-map-generic
  bandwidth remaining percent 5
  queue-limit 108 packets
 !
 class class-default
  bandwidth remaining percent 95
  queue-limit 2028 packets
 !
!
```

drop

To configure a traffic class to discard packets belonging to a specific class, use the **drop** command in policy-map class configuration mode. To disable the packet discarding action in a traffic class, use the **no** form of this command.

drop
no drop

Syntax Description This command has no arguments or keywords.

Command Default Disabled

Command Modes

Policy-map class configuration (config-pmap-c)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Examples

```
policy-map shape_GigabitEthernet0/0/1
  class class-default
   service-policy Branch-QoS-Policy
   shape average 1000000000
  !
  class class-default
    drop
  !
 !


policy-map type inspect test101
  class test101-seq-11-cm_
  drop
  !
```

flow-visibility

To enable flow visibility so that a router can perform traffic flow monitoring on traffic coming to the router from the LAN use the **flow-visibility** command. To disable the flow visibility use the **no** form of this command.

flow-visibility

no flow-visibility

Command Default Disabled.

Command Modes

Policy configuration (config-policy)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines Use the **show sdwan app-fwd cflowd** command to enable cflowd flow monitoring.

Examples

The following is an example of this command

```
Router(config)# policy
Router(config-policy)# flow-visibility
```

implicit-acl-logging

To configure your Cisco IOS XE Catalyst SD-WAN device to log dropped packets in the traffic, use the **implicit-acl-logging** command.

implicit-acl-logging

no implicit-acl-logging

Command Default

Logging is disabled.

Command Modes

Policy configuration (config-policy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

You can use these logs for security purposes; for example, to monitor the flows that are being directed to a WAN interface and to determine, in the case of a DDoS attack, which IP addresses to block.

When you enable implict ACL logging, by default, every 512th packet per flow is logged. It is recommended that you limit the number of packets logged, by including the **log-frequency** command in the configuration.

Log implicitly configured packets, logging every 512th packet per flow:

```
Router(config)# Policy
Router(config-policy)# implicit-acl-logging
```

inspect

To enable Cisco IOS stateful packet inspection, use the **inspect** command in policy-map-class configuration mode. To disable stateful packet inspection, use the **no** form of this command.

inspect
no inspect

Command Default

Cisco IOS stateful packet inspection is disabled.

Command Modes

Policy-map-class configuration (config-pmap-c)

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE inspect command.

Examples

The following example specifies inspection parameters and requests the **inspect** action with the specified inspect parameter:

```
policy-map type inspect mypolicy
 class type inspect inspect-traffic
  inspect
```

log (parameter-map type)

To log the firewall activity for an inspect parameter map, use the **log** command in parameter-map type inspect configuration mode.

log dropped-packets

Syntax Description

dropped-packets	Logs the packets dropped by the firewall.

Command Default

The firewall activity is not captured.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE log (parameter-map type) command.

Examples

The following example show how to configure the packets dropped by the firewall.

```
Router(config)# parameter-map type inspect-global
Router(config-profile)# alert on
Router(config-profile)# log dropped-packets
```

log flow-export

To log firewall events in NetFlow Version 9 format to an external netflow collector, use the **log flow-export** command in parameter-map type inspect-global configuration mode.

log flow-export

Syntax Description

v9	Specifies NetFlow Version 9 export as the export protocol.
udp	Configures the UDP connection.
destination	Specifies an IPv4 address destination.
ipv6-destination	Specifies an IPv6 address destination.
source	The source interface the device for HSL.

Command Modes

Parameter-map type inspect-global configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Examples

The following example show how to configure logging of of firewall events in NetFlow Version 9 format to an external IP address:

```
Device(config)# parameter-map type inspect-global
Device(config-profile)# log flow-export v9 udp destination 10.0.2.0 5000 vrf 1 source
GigabitEthernet0/0/5
Device(config-profile)# log flow-export v9 udp ipv6-destination 2001:DB8::1 vrf 65528 source
 GigabitEthernet0/0/3
```

log-frequency

To configure how often packet flows are logged, use the **log-frequency** command.

log-frequency *number*

Syntax Description

number	Logging Frequency: How often packet flows are logged. Range: Any positive integer value. While you can configure any positive integer value for the frequency, the software rounds the value down to the nearest power of 2. Default: 1000. With this default, the logging frequency is rounded down to 512. So, by default, every 512th packet per flow is logged. Maximum value: 2147483647

Command Default

Default logging frequency: 512

Command Modes

Policy configuration (config-policy)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

The following is an example of this command:

```
Router(config)# Policy
Router(config-policy)# implicit-acl-logging
Router(config-policy)# log-frequency 1000
```

match access-group

To configure the match criteria for a class map on the basis of the specified access control list (ACL), use the **match access-group** command in class-map configuration mode. To remove ACL match criteria from a class map, use the **no** form of this command.

match access-group name *access-group-name*
no match access-group name *access-group-name*

Syntax Description

name *access-group-name*	Named ACL whose contents are used as the match criteria against which packets are checked to determine if they belong to this class. The name can be a maximum of 40 alphanumeric characters.

Command Default

No match criterion is specified.

Command Modes

QoS class-map configuration (config-cmap)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco vManage CLI templates.

Examples

```
class-map type inspect match-all cmap
  match access-group name cmap
 !
```

multi-tenancy

To enable multi-tenancy as a global parameter map, use the **multi-tenancy** command in parameter-map type inspect configuration mode. To disable multi-tenancy as a global parameter map, use the **no** form of this command.

multi-tenancy

no multi-tenancy

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Parameter-map type inspect configuration (config-profile).

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines A parameter map allows you to specify parameters that control the behavior of actions and match criteria sthat are specified under a policy map and a class map respectively, for zone-based firewall policies.

Examples The following example shows how to enable multi-tenancy as a global parameter map:

```
Device(config)# parameter-map type inspect-global
Device(config-profile)# multi-tenancy
```

parameter-map type inspect-global

To configure a global parameter map and enter parameter-map type inspect configuration mode, use the **parameter-map type inspect-global** command in global configuration mode. To delete a global parameter map, use the **no** form of this command.

parameter-map type inspect-global
no parameter-map type inspect-global

Syntax Description This comand has no keywords or arguments.

Command Default Global parameter maps are not configured.

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines After you enter the **parameter-map type inspect-global** command, you can enter the commands listed in the table below in parameter-map type inspect-global configuration modes.

Command	Description
aggressive-aging	Enables aggressive aging of half-opened firewall sessions.
alert on	Enables Cisco IOS stateful packet inspection alert messages.

Command	Description
inspect	Enables and disables audit trail messages.
log {**dropped-packets** | **flow-export**}	Logs the dropped packets.
max-incomplete {**low** | **high**} *number-of-connections*	Defines the number of existing half-open sessions that will cause the software to start and stop deleting half-open sessions.
multi-tenancy	Enables Cisco vManage for multitenancy.
vpn zone security	Inspects traffic exchange between multiple service VPNs.

Ensure that you configure the **parameter-map type inspect-global** command with **vpn zone security** command to enable zone-based firewall.

For more information on usage guidelines, see the Cisco IOS XE parameter-map type inspect-global command.

Examples

The following example shows a sample parameter-map type inspect-global configuration:

```
Device(config)# parameter-map type inspect-global
Device(config)# alert on
Device(config-profile)# log dropped-packets
Device(config-profile)# multi-tenancy
Device(config-profile)# vpn zone security allow dia
```

policy

To enter policy configuration mode or configure policies, use the **policy** command in global configuration mode. To remove policy configurations, use the **no** form of this command.

policy [**access-list** | **app-visibility** | **class-map** | **cloud-qos-service-side** | **flow-visibility** | **flow-stickiness-disable** | **implicit-acl-logging** | **ipv6** | **lists** | **log-frequency** | **mirror** | **policer** | **qos-map** | **qos-scheduler** | **rewrite-rule** | **route-policy** | **utd-tls-decrypt**]
no policy [**access-list** | **app-visibility** | **class-map** | **cloud-qos-service-side** | **flow-visibility** | **implicit-acl-logging** | **ipv6** | **lists** | **log-frequency** | **mirror** | **policer** | **qos-map** | **qos-scheduler** | **rewrite-rule** | **route-policy** | **utd-tls-decrypt**]

Syntax Description

access-list	(Optional) Configures ACLs.
app-visibility	(Optional) Enables/disables application visibility.
class-map	(Optional) Configures class map.
cloud-qos	(Optional) Enables/Disables QoS for cEdge Cloud.
cloud-qos-service-side	(Optional) Enables/Disables QoS for cEdge Cloud on service side.
flow-visibility	(Optional) Enables/Disables flow visibility.
flow-stickiness-disable	(Optional) Enables/Disables flow stickiness.

implicit-acl-logging	(Optional) Enables/Disables logging of implicit acl packet drops.
ipv6	(Optional) Configures IPv6 policy.
lists	(Optional) Configures lists.
log-frequency	(Optional) Logs frequency as packet counts.
mirror	(Optional) Configures traffic mirror.
policer	(Optional) Configures policer.
qos-map	(Optional) Configures QoS map.
qos-scheduler	(Optional) Configures QoS scheduler.
rewrite-rule	(Optional) Configures rewrite rule.
route-policy	(Optional) Configures route policies
utd-tls-decrypt	(Optional) Configures TLS Decryption policies.

Command Default

Default behavior or values vary based on optional arguments or keywords.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.
Cisco IOS XE Release 17.6.1a	The **flow-stickiness-disable** keyword is added.
Cisco IOS XE Catalyst SD-WAN Release 17.13.1a	The **flow-stickiness-disable** keyword is added for NAT66 DIA.

Usage Guidelines

Policy influences the flow of data traffic and routing information among Cisco devices in the overlay network. This command can be used to enter the policy configuration mode where further configurations can be done or to configure policies with optional arguments or keywords.

Example

The following example enters the policy configuration mode. It defines a policer profile named pol1 and sets the burst size to 15,000 bytes, and rate to 500,000,000 bps, and configures to drop the traffic if the burst size or traffic rate is exceeded.

```
Device(config)# policy
Device(config-policy)# policer pol1
Device(config-policy-pol1)# burst 15000
Device(config-policy-pol1)# rate 500000000
Device(config-policy-pol1)# exceed drop
Device(config-policy-pol1)# flow-stickiness disable
```

The following example enables app-visibility.

```
Device(config)# policy app-visibility
```

The following example disables flow-stickiness.

```
Device(config-policy)# flow-stickiness disable
```

policy-map type inspect

To create a Layer 3 and Layer 4 or a Layer 7 (protocol-specific) inspect-type policy map, use the **policy-map type inspect** command in global configuration mode. To delete an inspect-type policy map, use the **no** form of this command.

Layer 3 and Layer 4 (Top Level) Policy Map Syntax
policy-map type inspect *policy-map-name*
no policy-map type inspect *policy-map-name*

Layer 7 (Application-Specific) Policy Map Syntax
policy-map type inspect *protocol-name policy-map-name*
no policy-map type inspect *protocol-name policy-map-name*

Syntax Description

policy-map-name	Name of the policy map. The name can be a maximum of 40 alphanumeric characters.
protocol-name	Layer 7 application-specific policy map. The supported protocol is: **avc** —Firewall AVC-based poilcy map.

Command Default

No policy map is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE policy-map type inspect command.

Examples

```
policy-map type inspect avc aa1-pm_
! first
class aa1-cm0_
deny
```

service-policy (zones)

To attach a Layer 7 policy map to a top-level policy map, use the **service-policy** command in zone-pair configuration mode. To delete a Layer 7 policy map from a top-level policy map, use the **no** form of this command.

service-policy *policy-map-name*
no service-policy *policy-map-name*

Syntax Description

policy-map-name	Name of the Layer 7 policy map to be attached to a top-level policy map.

Command Default

None

Command Modes

Zone-pair configuration

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE service-policy (zones) command.

Examples

```
policy-map type inspect test
class test-seq-1-cm_
inspect audit-trail-pmap_
service-policy avc aa1-pm_
!
```

service-policy type inspect

To attach a firewall policy map to a zone-pair, use the **service-policy type inspect** command in zone-pair configuration mode. To disable this attachment to a zone-pair, use the **no** form of this command.

service-policy type inspect *policy-map-name*
no service-policy type inspect *policy-map-name*

Syntax Description

policy-map-name	Name of the policy map. The name can be a maximum of 40 alphanumeric characters.

Command Default

None

Command Modes

Zone-pair configuration (config-sec-zone-pair)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE service-policy type inspect command.

Examples

The following example defines zone-pair LAN-WAN and attaches the service policy test-policy to the zone-pair:

```
!
zone security LAN
vpn 2
!
zone security WAN
vpn 0
!
zone-pair security ZP_LAN_WAN_test-policy source LAN destination WAN
 service-policy type inspect test-policy
!
```

vpn zone security

To enable vpn zone security globally, use the **vpn zone security** command under the **parameter-map type inspect-global** command mode for inspecting traffic between zones. To remove the vpn zone security, use the no form of the command under the parameter-map type inspect-global configuration mode.

vpn zone security

no vpn zone security

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command is qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Zone-based firewall feature can be enabled on Cisco IOS XE Catalyst SD-WAN devices for inspecting traffic exchange between multiple service VPNs. This feature can be globally enabled by using the vpn zone security command under parameter-map type inspect-global command.

Examples

The following example shows enabling zone based firewall feature globally:

```
Device(config)# parameter-map type inspect-global
Device(config-profile)# vpn zone security
```

Related Commands

Command	Description
zone security	Defines a security zone.
zone-pair security	Defines a zone pair on which to implement the zone security firewall feature.

vpn (zone)

To associate a vpn with a zone , use the **vpn** *id* command under the **zone security** command. To disassociate a vpn id, use the **no** form under the **zone security** mode.

vpn *id*
no vpn *id*

Syntax Description

id	Specifies the id of a vrf configured on a Cisco IOS XE Catalyst SD-WAN device.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Zone-based firewall feature can be enabled on Cisco IOS XE Catalyst SD-WAN devices for inspecting traffic exchange between multiple service VPNs. This feature can be globally enabled by using the vpn zone security command under parameter-map type inspect-global command.

Examples

The following example shows how to associate vpn 32 with zone corporate:

```
Device(config)# zone security corporate
Device(config-sec-zone)# vpn 32
```

Related Commands

Command	Description
zone-pair security	Defines a zone-pair on which to implement the zone security firewall feature.

zone pair security

To create a zone pair, use the **zone-pair security** command in global configuration mode. To delete a zone pair, use the **no** form of this command.

zone-pair security *zone-pair-name* **source** [*source-zone-name* | **self**] **destination** [*destination-zone-name* | **self**]
no zone-pair security *zone-pair-name* **source** [*source-zone-name* | **self**] **destination** [*destination-zone-name* | **self**]

Syntax Description

zone-pair-name	Name of the zone being attached to an interface. You can enter up to 128 alphanumeric characters.
source *source-zone-name*	Specifies the name of the router from which traffic is originating.
destination *destination-zone-name*	Specifies the name of the device to which traffic is bound.
self	Specifies the system-defined zone. Indicates whether traffic will be going to or from a device.

Command Default

A zone pair is not created.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE zone-pair security command.

Examples

The following example shows how to create zones LAN and WAN, identify them, and create a zone pair where LAN is the source and WAN is the destination:

```
zone security LAN
vpn 2
!
zone security WAN
vpn 0
!
```

The following example shows how to define zone pair LAN-WAN and attach a service policy, test-policy to the zone-pair:

```
zone-pair security ZP_LAN_WAN_test-policy source LAN destination WAN
  service-policy type inspect test-policy
```

zone security

To create a security zone, use the **zone security** command in global configuration mode. To delete a security zone, use the **no** form of this command.

zone security *zone-name*
no zone security *zone-name*

Syntax Description

zone-name	Name of the security zone. You can enter up to 256 alphanumeric characters.

Command Default

There is a system-defined "self" zone.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Note The self zone does not require any declaration.

For usage guidelines, see the Cisco IOS XE zone security command.

Examples

The following example shows how to create and describe zones LAN and WAN:

```
zone security LAN
 vpn 2
!
zone security WAN
 vpn 0
!
```