

# Configure Packet Duplication Using Policy Groups in SD-WAN

## Contents

---

### [Introduction](#)

### [Prerequisites](#)

[Requirements](#)

[Components Used](#)

### [Background Information](#)

[Packet Duplication](#)

[Packet Duplication Workflow](#)

### [Configure](#)

[Network Diagram](#)

### [Configure Packet Duplication Using Policy Groups](#)

[Step 1. Configure Application Priority & SLA Policy](#)

[Step 2. Define Policy Groups](#)

### [Verify](#)

[Monitor Packet Duplication Statistics from the SD-WAN edge router's CLI](#)

[Monitor Packet Duplication Statistics from the Cisco Catalyst SD-WAN Manager](#)

### [Related Information](#)

---

## Introduction

This document describes Packet Duplication configuration in Software-Defined Wide-Area Networks (SD-WAN).

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of general topics related to Cisco Catalyst Software-Defined Wide Area Network (SD-WAN).

### Components Used

The information in this document is based on:

- Cisco Catalyst SD-WAN Manager version 20.15.3.
- Cisco IOS® XE Catalyst SD-WAN Edges version 17.15.3a

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

# Background Information

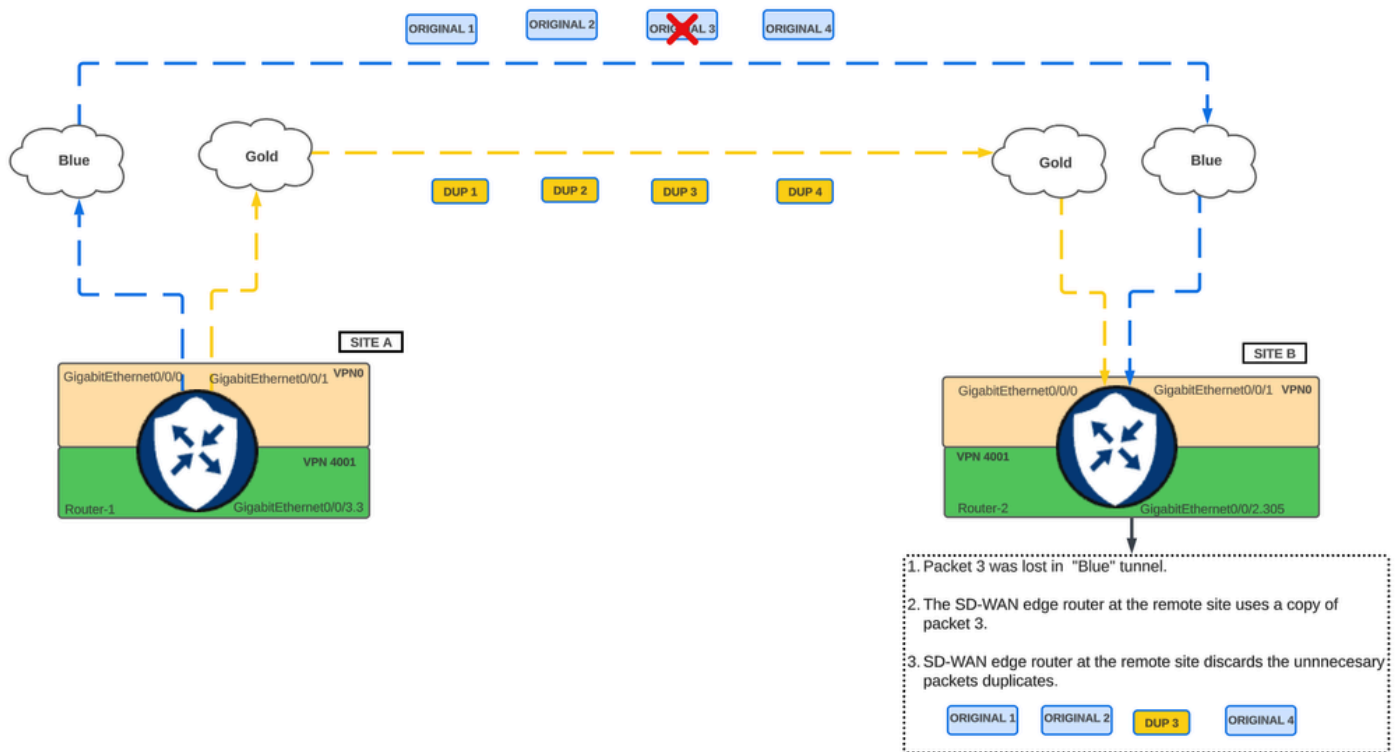
## Packet Duplication

Packet duplication is an SD-WAN feature designed to ensure reliability and reduce packet loss for time-sensitive applications (such as Voice over IP (VoIP), video conferencing, financial transactions and Mission-Critical control systems) in networks where a SD-WAN edge router has multiple overlay IPsec tunnels to the next-hop router.

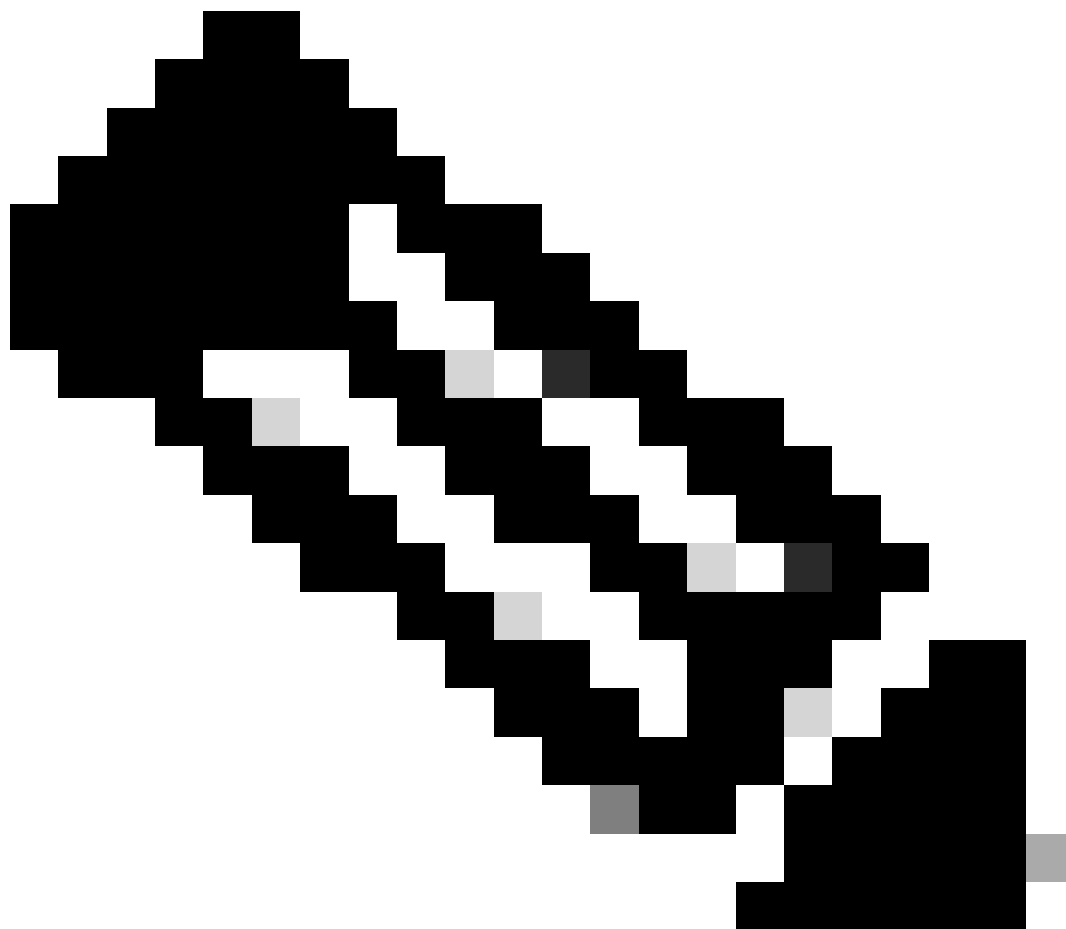
When Packet Duplication is enabled, the SD-WAN edge router **creates duplicate packets** and transmits them simultaneously over **another active IPsec tunnel**.

## Packet Duplication Workflow

1. The SD-WAN edge router creates duplicate copies of the outbound packet.
2. The duplicated packets are transmitted simultaneously over another tunnel IPsec tunnel.
3. If a packet is lost over one path, the SD-WAN edge router at remote site, processes a copy of the same packet received over another tunnel.
4. If no packets are lost, the SD-WAN edge router at the remote site discards the unnecessary packets duplicates.

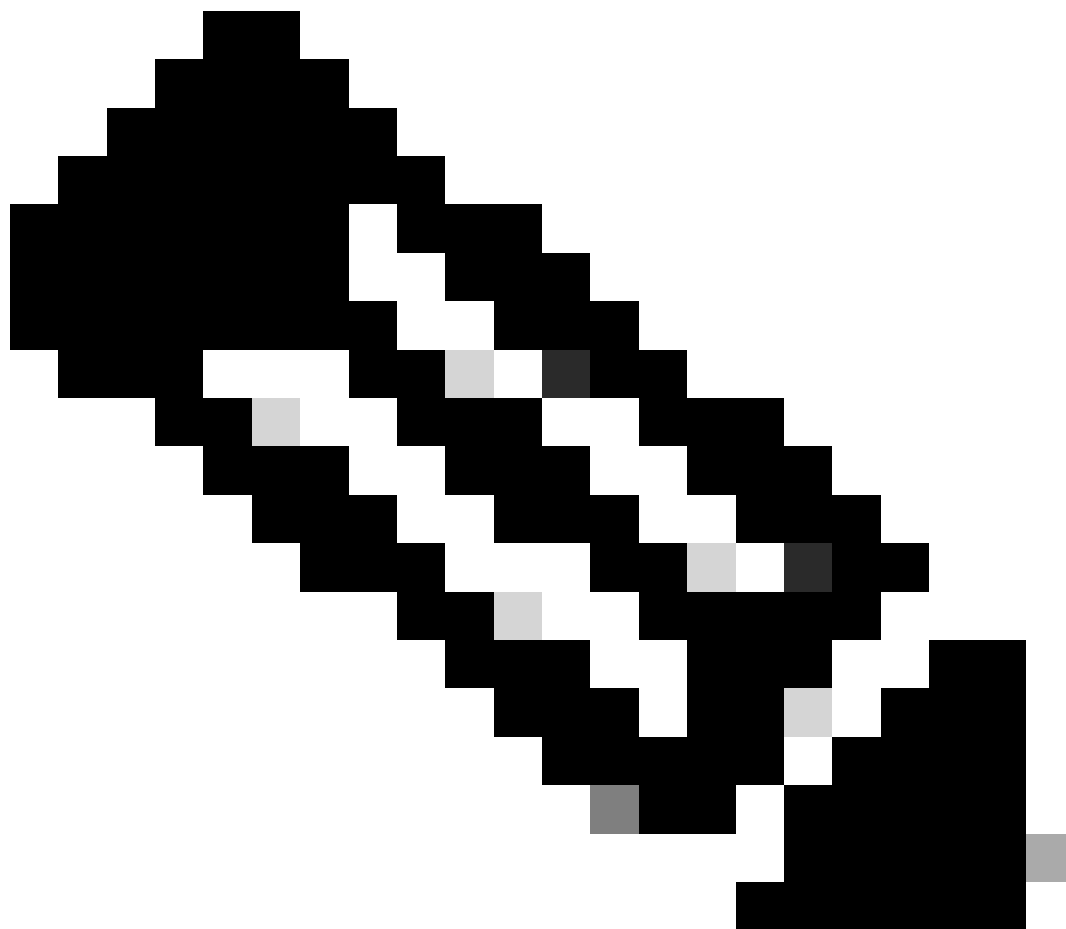


Packet Duplication workflow



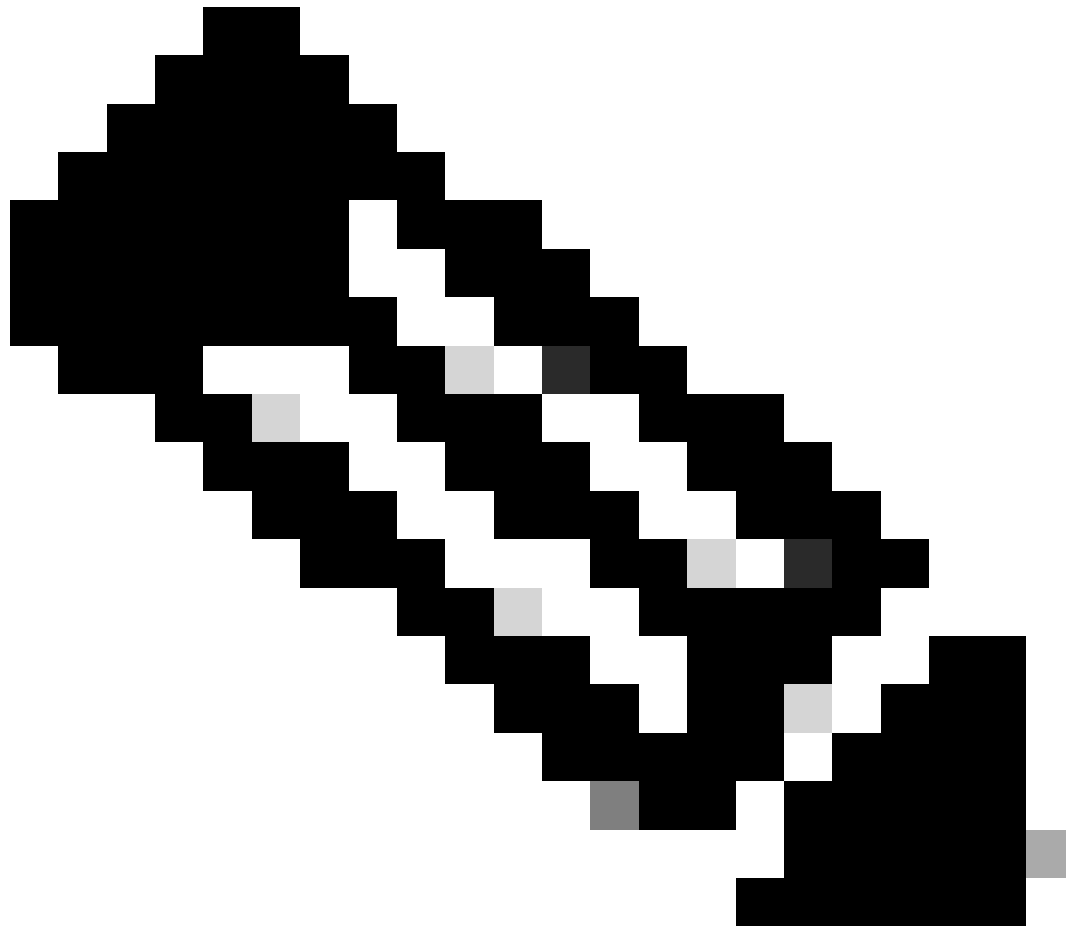
**Note:** Packet Duplication is only supported in topologies where SD-WAN edge routers establish at least two overlay IPsec tunnels between the local site to the remote site.

---



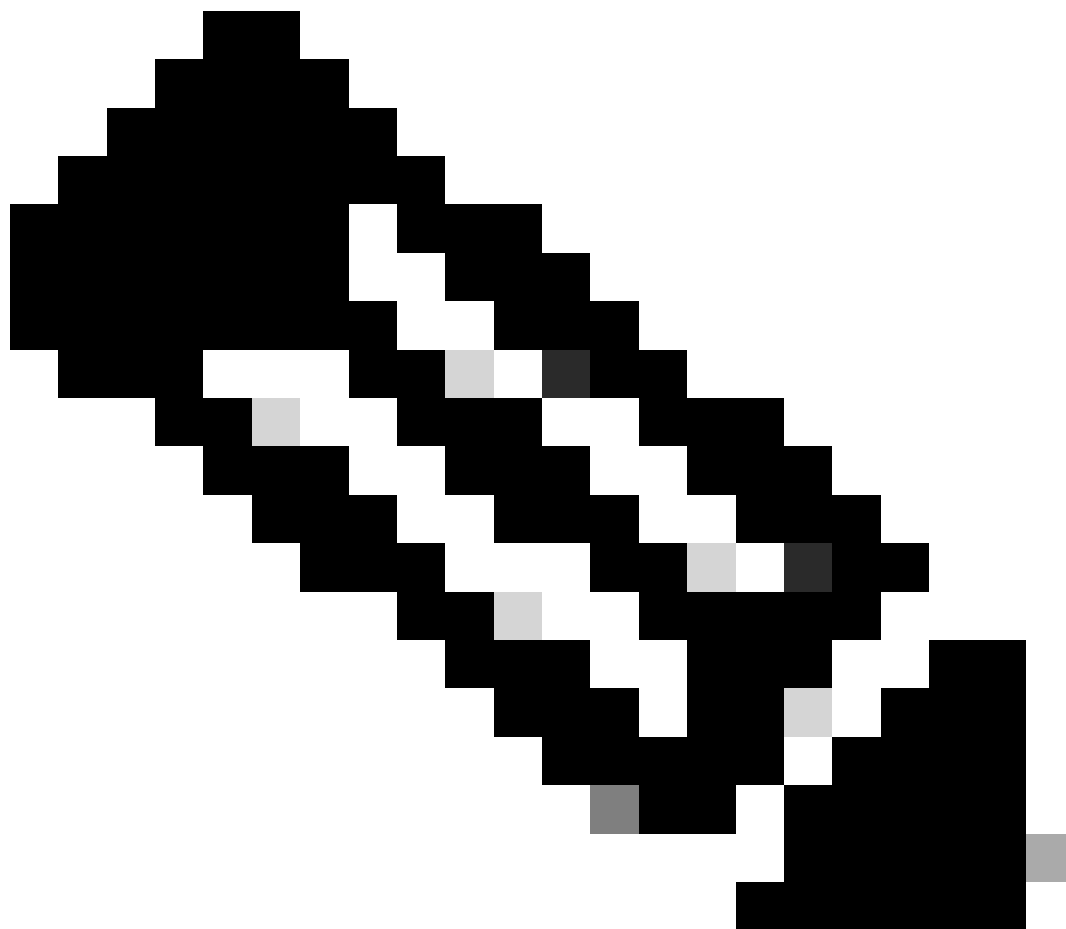
**Note:** Data Policy and Application-Aware Routing (AAR) must not be applied to packet-duplicated traffic.

---



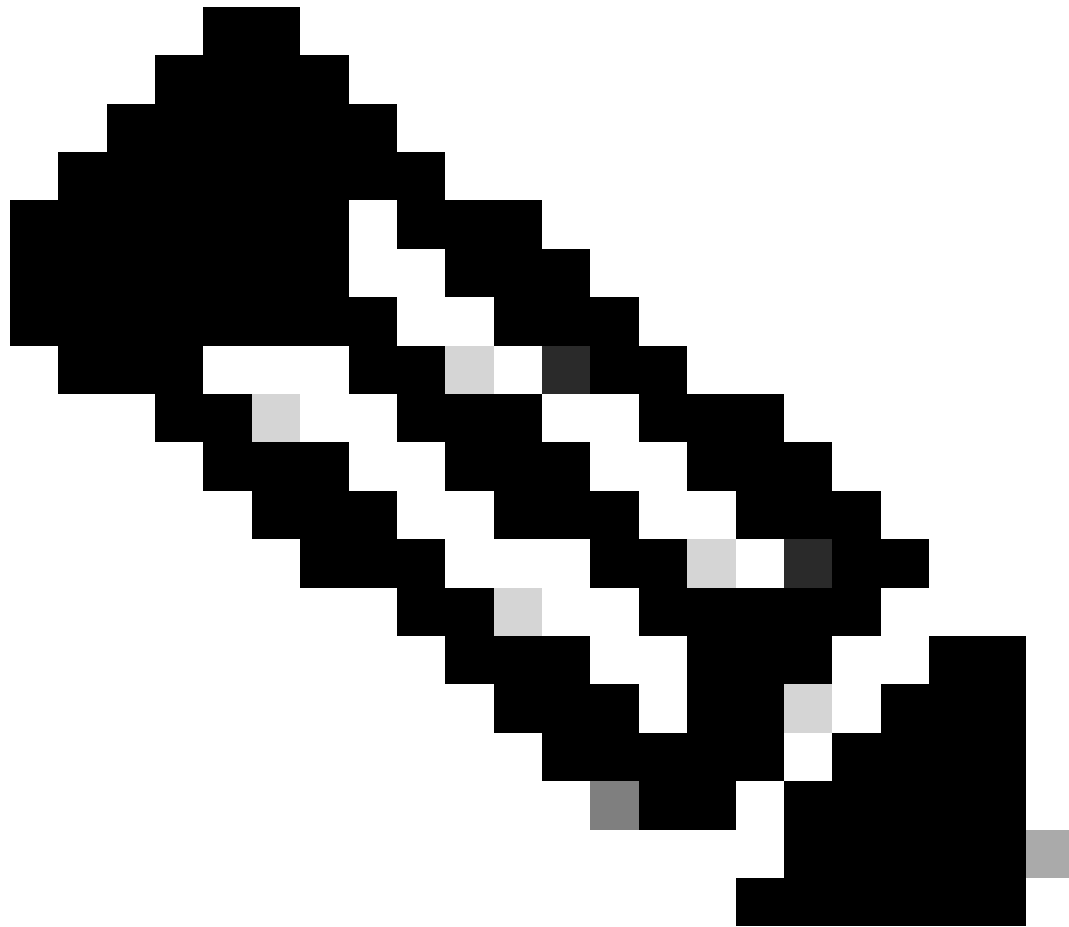
**Note:** Packet duplication interop, forward error correction (FEC), and TCP optimization on Cisco IOS XE Catalyst SD-WAN devices is not supported between Cisco IOS XE Release 16.x and Cisco IOS XE Catalyst SD-WAN Release 17.x versions.

---



**Note:** Packet duplication is supported only on Cisco IOS XE Catalyst SD-WAN devices.

---

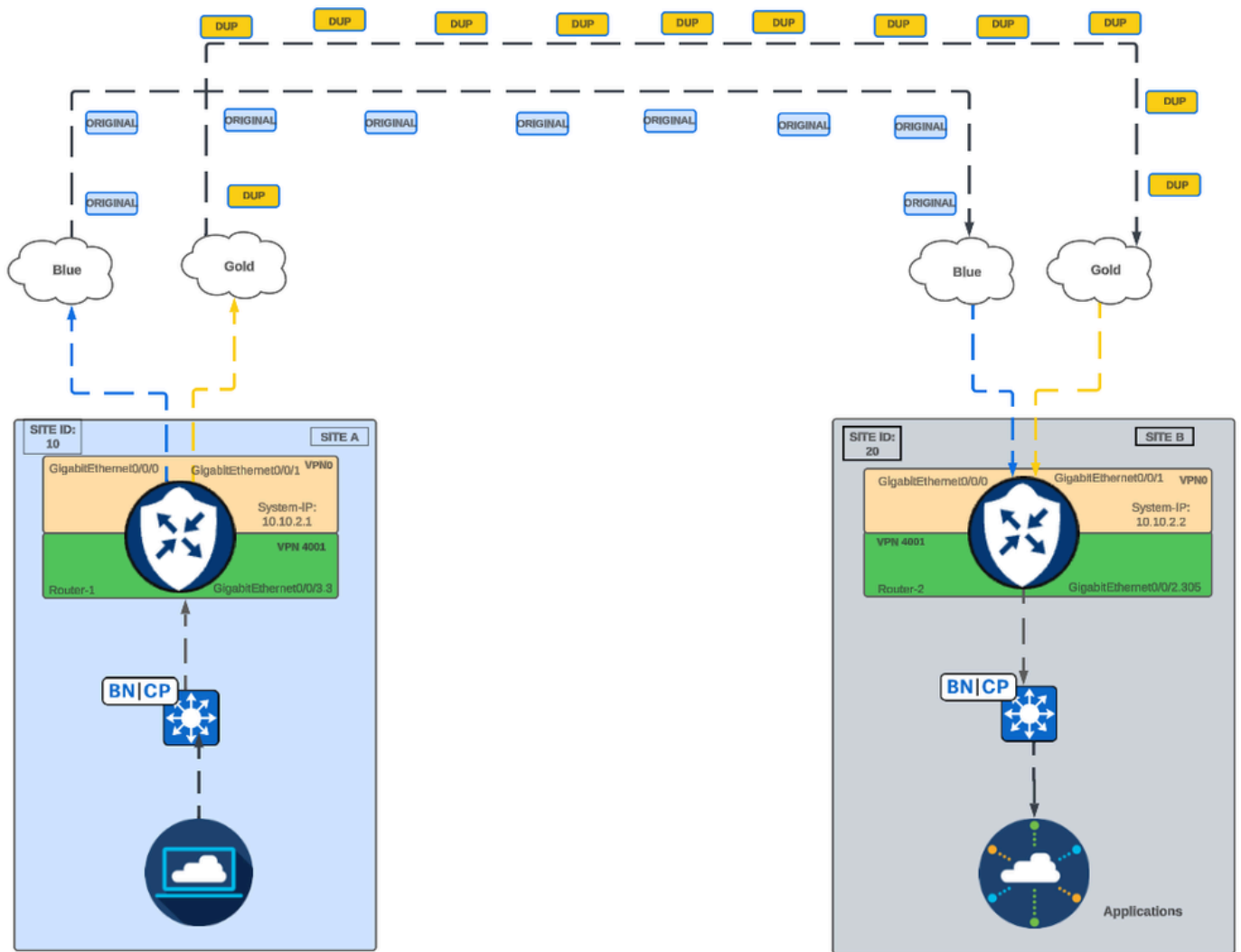


**Note:** When packets are intercepted for duplication, the system queries the IP database using the incoming tunnel ID. It then fetches the duplicate tunnel object. The system compares the packet length with the path maximum transmission unit (PMTU) of the duplicate tunnel. If the packet length is smaller than the duplicate tunnel's PMTU, the packets are duplicated.

---

## Configure

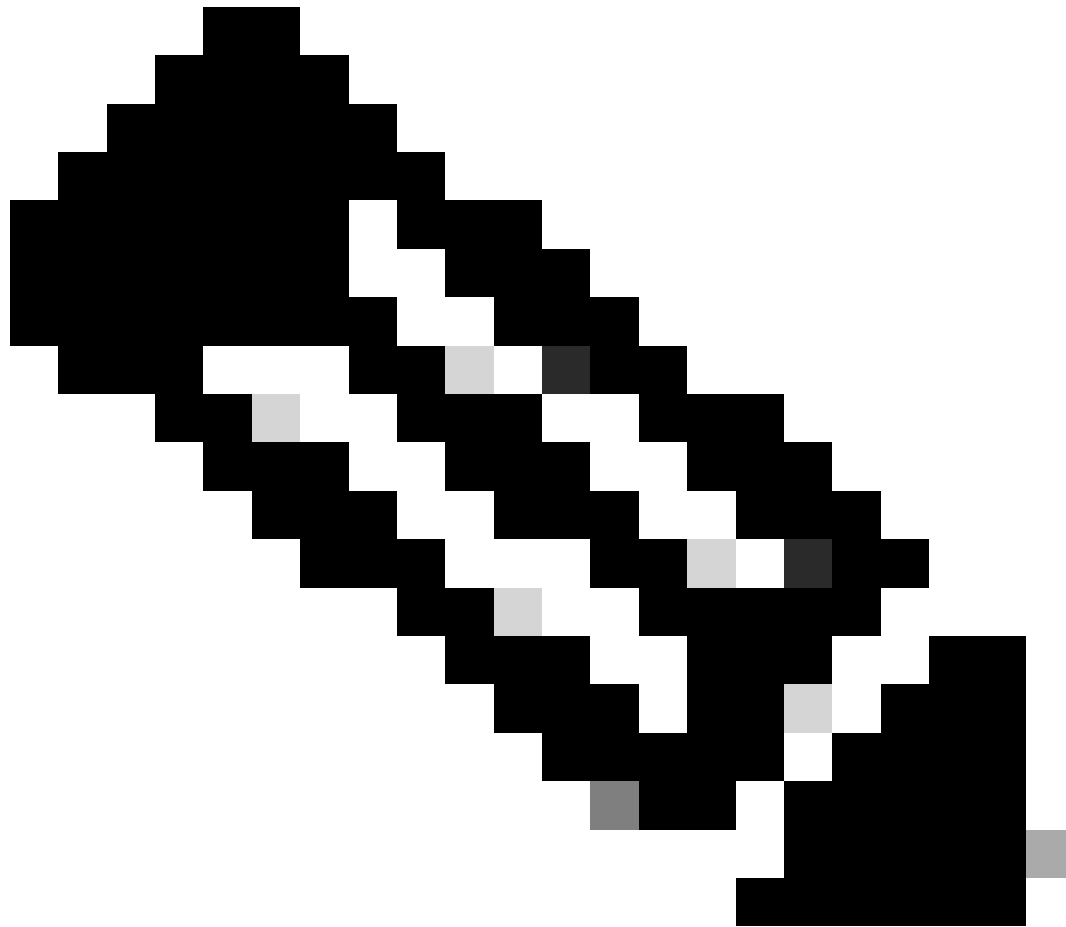
### Network Diagram



Site-to-Site Network Diagram

## Configure Packet Duplication Using Policy Groups





**Note:** Minimum supported release: Cisco Catalyst SD-WAN Control Components Release 20.14.1

---

## Step 1. Configure Application Priority & SLA Policy

- Log in to Cisco Catalyst SD-WAN Manager GUI.
- Navigate to **Configuration > Policy Groups > Application Priority & SLA > Add Application Priority & SLA Policy**.
- Configure **Application Priority & SLA Policy** name > Click on **Create**.

**Policy Groups**

Configuration | Policy Group 0 | **Application Priority & SLA 0** | NGFW 0 | Secure Internet Gateway / Secure Service Edge 0 | DNS Security 0

**Application Priority & SLA Policy**

Policy Name  
packet\_duplication\_tz

Description(optional)

Cancel Create

*Application Priority & SLA Policy name*

- Enable **Advanced Layout** in the top right pane > Click on **Add Traffic Policy**.

Cisco Catalyst SD-WAN

Policies > Application Priority & SLA

packet\_duplication\_tz

Additional Settings | Advanced Layout ☒

Change made in advanced view won't save to simple view.

+ Add Traffic Policy

SLA Class | QoS Queue

No SLA Class added, add your first SLA Class in Traffic Policy

*Advance Layout*

- Configure **Traffic PolicyName**, service **VPN(s)** and **Direction**.
- Identify **Default Action** > Select **Accept** > Click on **Add**

### Add Traffic Policy List

Policy Name  
packet\_duplication\_tz\_traffic\_policy

VPN(s)  
4001

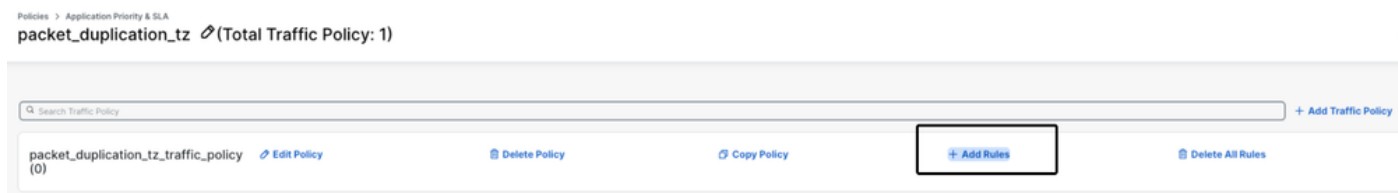
Direction  
Service

Default Action  
☒ Accept ☐ Drop

Cancel Add

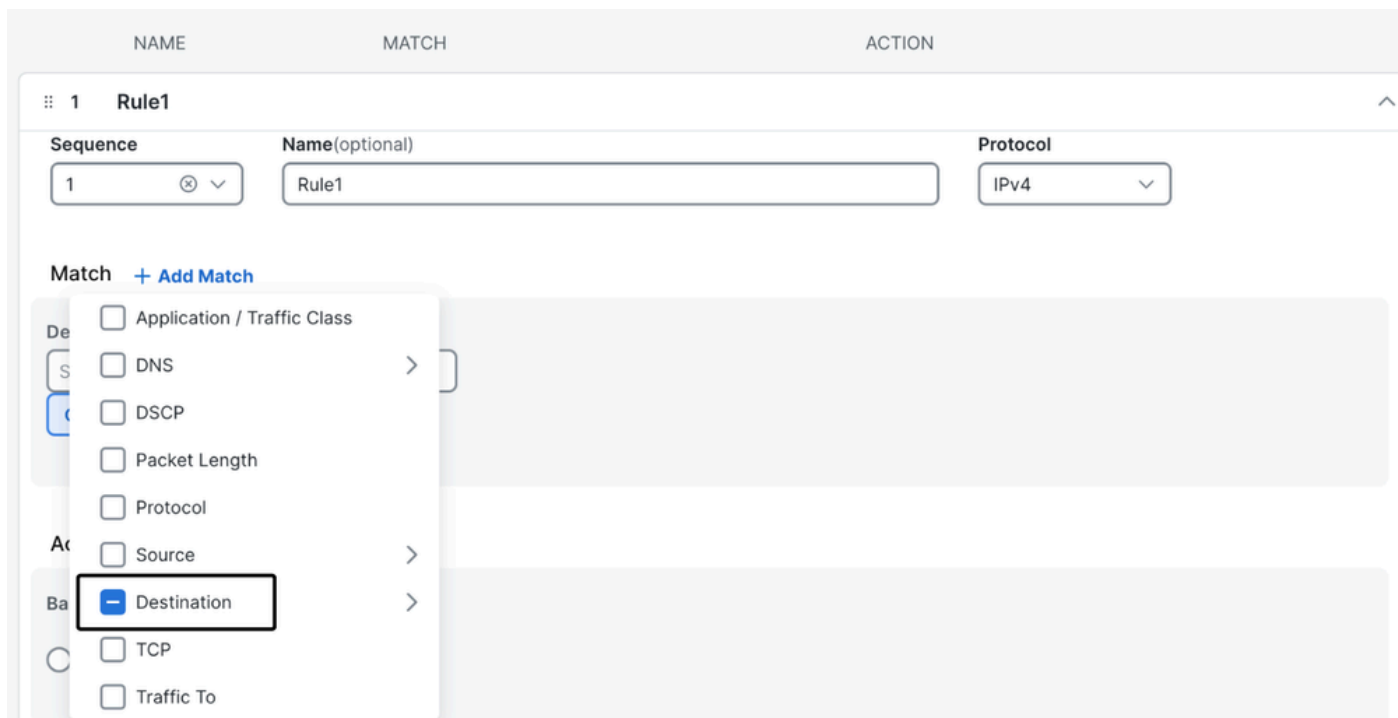
*Traffic Policy name*

- Click on **Add Rules**

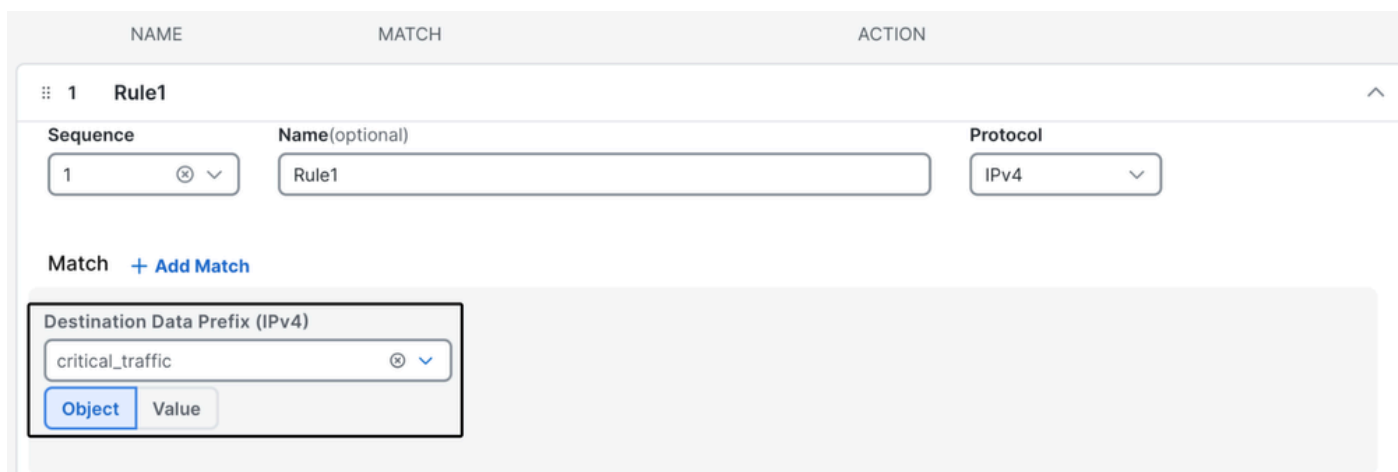


*Add Rules*

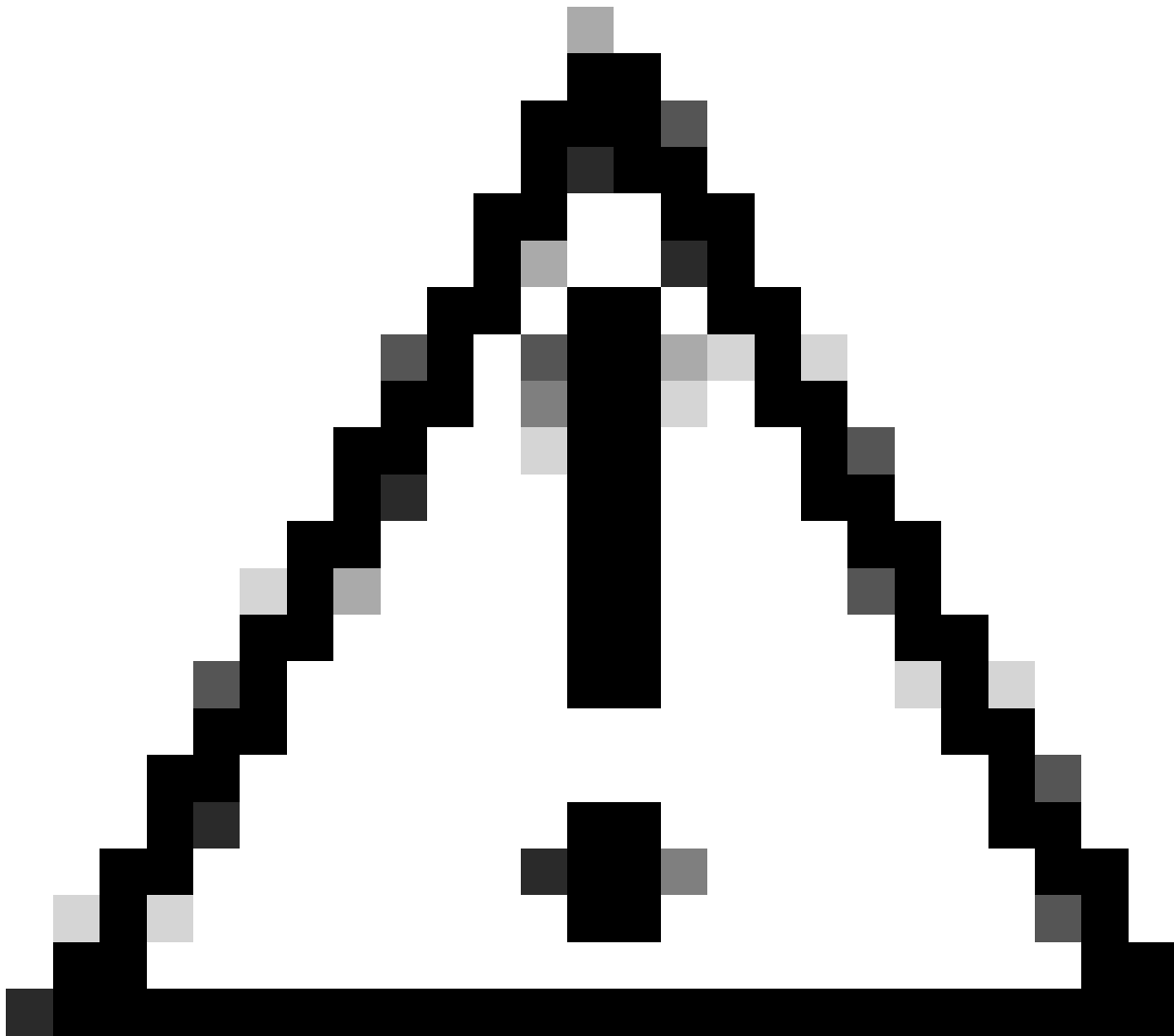
- Click on **Add Match** > Select a match condition.



*Match conditions*



*Destination Data Prefix*



**Caution:** Packet Duplication in SD-WAN is intended for use with critical applications or critical traffic. Enabling this feature for all traffic types is not recommended, as it results in increased CPU load and potential performance degradation on the SD-WAN edge router. During this laboratory test, CPU usage went up by about 10%.

---



**Note:** This laboratory uses the Destination Data Prefix as a match condition. Additionally, the Cisco Catalyst SD-WAN Manager supports the use of Applications or Application Family Lists, if required.

- 
- Identify **Action**
  - Select **Accept** > Click on **Add Action** > Select **Loss Correction**

Match [+ Add Match](#)

Destination Data Prefix (IPv4)

critical\_traffic

[Object](#) [Value](#)

Action [+ Add Action](#)

- ☐ Remote Preferred Color
- ☐ Preferred Color group
- ☐ NAT Pool
- ☐ NAT VPN
- ☐ Next Hop
- ☐ Policer
- ☐ Redirect DNS
- ☐ TLOC
- ☐ Service
- ☐ Service Chain
- ☐ Secure Internet Gateway / Secure Service Edge
- ☐ AppQoS Optimization
- ☒ Loss Correction

: 1 / 1

Add Action

- Select **Packet Duplication** > Click on **Save Match and Actions** > Click on **Save**

Action [+ Add Action](#)

Base Action

☒ Accept ☐ Drop

Loss Correction

Type

Select one Type ^

FEC Adaptive

FEC Always

Packet Duplication

Cancel

Save Match and Actions

*Select Packet Duplication*

## Step 2. Define Policy Groups

- Navigate to **Policy Group** > Click on **Add Policy Group**
- Configure **Policy Group Name** and **Solution** > Click on **Create**

### Add Policy Group

Policy Group Name

packet\_duplication\_policy\_group\_tz

Solution

sdwan

Description(optional)

Cancel

Create

*Define Policy Groups*

- Identify **Application Priority**
- Select **Application Priority & SLA Policy** created > Click on **Save**

Policy Group 1 Application Priority & SLA 1 NGFW 0 Secure Internet Gateway / Secure Service Edge 0 DNS Security 0

+ Add Policy Group Export Import As of: June 25, 2025 at 2:09 PM

Q Search

Name	Description	Number of Policies	Number of Devices	Devices Up to Date	Updated By	Last Updated On	Actions
packet_duplication_policy_grou...							
Policy Group Name	Description(optional)						
packet_duplication_policy_group_tz							
Application Priority	NGFW						
Please Select one	Please Select one						
packet_duplication_tz							
	DNS Security						
	Please Select one						
		Device Solution Type sdwan Deployment Associated + Add Save Deploy					
Create New							

Select Application Priority & SLA Policy

- Associate the SD-WAN edge routers where packet duplication is to be enabled.
- Identify **Associated** > Click on **Add**
- Click on **Associated Devices** > Choose Devices > Click on **Associated Devices**

Name	Description	Number of Policies	Number of Devices	Devices Up to Date	Updated By	Last Updated On	Actions
packet_duplication_policy_grou...							
Policy Group Name	Description(optional)						
packet_duplication_policy_group_tz							
Application Priority	NGFW						
packet_duplication_tz	Please Select one						
Secure Internet Gateway / Secure Service Edge	DNS Security						
Please Select one	Please Select one						
		Device Solution Type sdwan Deployment Associated + Add Save Deploy					

Associated devices

Devices (0)

Q Search Table

0 selected Associate Devices Remove Devices Change Device Values Deploy Export As of: Jun 25, 2025 02:17 PM

Chassis Numbers	Site Name	Hostname	Tags	Config Locked	System IP	Site ID	Device Status	Added by Rule
-----------------	-----------	----------	------	---------------	-----------	---------	---------------	---------------

Associate Devices

**Summary**  
Review the information for the devices to be added. You can deploy the devices now or later.

Choose devices

Devices To Be Added (1)

Edit

Chassis Number	Device Model	Hostname	Config Group	System IP	Site ID	Serial No./Token	Config Locked
C8500-12X4QC-TTM2729020Q	C8500-12X4QC	Router	test-cll	10.10.10.1	10	05328431376678528AE1	Yes

Items per page: 25 1 - 1 of 1

Devices to be associated



- Click on **Provision Devices** > Select **Devices to Deploy** > Click on **Deploy**

## ✔ Do you want to provision devices in packet\_duplication\_policy\_group\_tz?

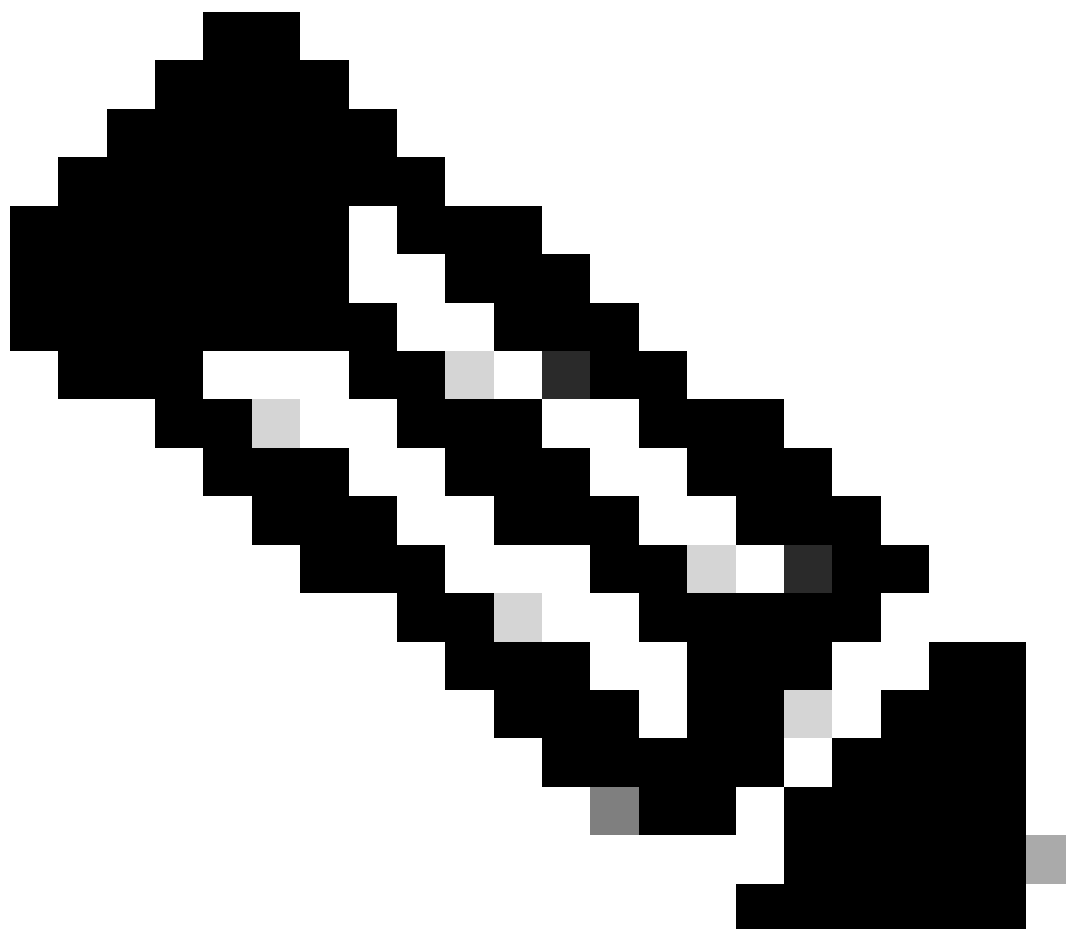
Devices added to policy group packet\_duplication\_policy\_group\_tz!

No, I Will Do It Later

Provision Devices

*Provision Devices*

---



**Note:** A Configuration Group needs to be associated with the SD-WAN edge router before deploying a Policy Group.

---

## Verify

**Monitor Packet Duplication Statistics from the SD-WAN edge router's CLI**



**Note:** A SD-WAN data policy has been used to configure packet duplication on the Cisco Catalyst SD-WAN Controller and the configuration has been pushed to the SD-WAN edge router.

---

Run the command **show sdwan policy from-vsmart** to display the data policies that have been sent from the Cisco Catalyst SD-WAN controller to the SD-WAN edge router.

```
<#root>
```

```
Router#
```

```
show sdwan policy from-vsmart
```

```
from-vsmart data-policy data_service_packet_duplication_tz
```

```
direction from-service
```

```
vpn-list vpn_packet_dup_4001
```

```
sequence 1
```

```
match
source-data-prefix-list critical_traffic

action accept
```

```
loss-protection packet-duplication
```

```
default-action accept
from-vsmart lists vpn-list vpn_packet_dup_4001
vpn 4001
from-vsmart lists data-prefix-list critical_traffic
ip-prefix 0.0.0.0/0
```

Run the command **show sdwan tunnel statistics pkt-dup** to display statistics related to packet duplication in SD-WAN transport tunnels.

```
<#root>
```

```
Router#
```

```
show sdwan tunnel statistics pkt-dup
```

```
tunnel stats ipsec 10.0.20.15 10.0.21.16 12346 12386
pktdup-rx          0

pktdup-rx-other 56
```

```
<<<< Duplicate packets were received on the Secondary tunnel
```

```
pktdup-rx-this  0
pktdup-tx       0
```

```
pktdup-tx-other 56 <<<< Duplicate packets were sent from the Secondary tunnel
```

```
pktdup-capable  true
```

```
tunnel stats ipsec 10.1.15.15 10.1.16.16 12346 12366
```

```
pktdup-rx          56 <<<< Original packets were received on the primary tunnel
```

```
pktdup-rx-other 0
```

```
pktdup-rx-this  56
```

```
<<<< Duplicate packets were received on secondary tunnel but counted in the primary tunnel statistics
```

```
pktdup-tx          56 <<<< Original packets sent from primary tunnel
```

```
pktdup-tx-other 0
```

```
pktdup-capable true
```

<<<< Capability exchange with other edge routers

Run the command **show sdwan bfd sessions** to display the status and statistics of BFD sessions between SD-WAN edge routers.

<#root>

Router#

```
show sdwan bfd sessions
```

SYSTEM IP	SITE ID	STATE	SOURCE TLOC COLOR	REMOTE TLOC COLOR	SOURCE IP	DST PUBLIC IP	DST PUBLIC IP	DETECT TX	PO
10.10.2.2	10	up	gold	gold	10.0.20.15	10.0.21.16			12
10.10.2.2	10	up	blue	blue	10.1.15.15	10.1.16.16			12

Run the command **show platform hardware qfp active feature bfd datapath sdwan summary** to display the statistics at the hardware/data plane level, for IPSEC SD-WAN tunnels.

<#root>

Router#

```
show platform hardware qfp active feature bfd datapath sdwan summary
```

Total number of session:

LD

	SrcIP	DstIP	TX	RX	Encap	State	AppProbe	AdjId
20024								
	10.0.20.15	10.0.21.16	1057739	1057489	IPSEC	Up	YES	GigabitEthernet0/0/1 (0xf

<<< Identify LD's number that uses the gold color

20028

10.1.15.15	10.1.16.16	1057782	1057494	IPSEC	Up	YES	GigabitEthernet0/0/0 (0xf
------------	------------	---------	---------	-------	----	-----	---------------------------

<<<

Identify LD's number that uses the blue colo

r

Run the command **show platform hardware qfp active feature sdwan client sysip summary** to display a **summary of the system IP addresses (sysip)** associated with the SD-WAN client feature, as processed by

the Quantum Flow Processor (QFP).

TunID = Tunnel ID of the primary local SD-WAN tunnel (based on the last 2 digits of LD)

DupID = TheDuplication ID of the secondary local SD-WAN tunnel (based on the last 2 digits of LD)

<#root>

Router#

show platform hardware qfp active feature sdwan client sysip summary

SysIP - SiteID - Next -

TunID

-

DupID

- BfdDis - BfdSta - LocCo - RemCo - Encap - feC - mtu

10.10.2.2 10 0

24

28

20024	UP	1	1	IPSEC	352	1442
10.10.2.2	10	0				

28

24

20028	UP	2	2	IPSEC	352	1442
-------	----	---	---	-------	-----	------

Run the command **show platform hardware qfp active feature sdwan data sysip summary** to display a **summary of SD-WAN system IPs** in the data plane.

TunID = Tunnel ID of the primary local SD-WAN tunnel (based on the last 2 digits of LD)

DupID = TheDuplication ID of the secondary local SD-WAN tunnel (based on the last 2 digits of LD)

<#root>

Router#

show platform hardware qfp active feature sdwan data sysip summary

BktIdx	BktAddr	SysIP	SiteID	Next	on-demnd	Gleaning	glean_ipc_paks
Idx							

TunID

DupID

	bfdDisc	bfdState	locCo1	remCo1	Encap	feC	mtu	sess-ppe
77	0x6a9a4c60							
10.10.2.2								
0	10	0x0	No	No		0		
24								
28								
1	20024	3	1	1	IPSEC	352	1442	0x6934f1a0
28								
24								
	20028	3	1	17	IPSEC	352	1442	0x6934f1e0

Additional commands to review CPU utilization:

<#root>

Router#

```
show processes cpu platform sorted | include CPU
```

Router##

```
show platform resources
```

Router#

```
show processes cpu history
```

## Monitor Packet Duplication Statistics from the Cisco Catalyst SD-WAN Manager

- From the Cisco SD-WAN Manager menu, choose **Monitor > Devices**
- Choose a device.
- For a device, in the **Action** column, click "...". and choose **Real Time**.
- In the Device Options drop-down menu and choose **Tunnel Packet Duplication Statistics**.

Device Options:

🔍 Tunnel Packet Duplication Statistics

🔍 Search

Total Rows: 5  

Hostname	TUNNEL PROTOCOL	SOURCE IP	DEST IP	SOURCE PORT	DEST PORT	PKTDUP RX	PKTDUP RX OTHER	PKTDUP RX THIS	PKTDUP RX FWD
Router	ipsec	10.0.20.15	10.0.21.16	12346	12386	0	56	0	0
Router	ipsec	10.1.15.15	10.1.16.16	12346	12366	56	0	56	0

PKTDUP TX	PKTDUP TX OTHER	PKTDUP TX TUN SELECTION FAIL	PKTDUP TX TUN SEND FAIL	PKTDUP CAPABLE
0	56	0	0	true
56	0	0	0	true

Packet Duplication statistics

## Related Information

- [Packet Duplication](#)
- [Policy Groups](#)
- [Cisco Catalyst SD-WAN Configuration Groups](#)