

SD-WANのポリシーグループを使用したパケット複製の設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[パケットの重複](#)

[パケット複製のワークフロー](#)

[設定](#)

[ネットワーク図](#)

[ポリシーグループを使用したパケット複製の設定](#)

[ステップ 1: アプリケーションの優先度とSLAポリシーの設定](#)

[ステップ 2: ポリシーグループの定義](#)

[確認](#)

[SD-WANエッジルータのCLIからのパケット複製統計情報の監視](#)

[Cisco Catalyst SD-WAN Managerからのパケット重複統計情報の監視](#)

[関連情報](#)

はじめに

このドキュメントでは、ソフトウェア定義型ワイドエリアネットワーク(SD-WAN)でのパケット複製(PD)の設定について説明します。

前提条件

要件

Cisco Catalyst Software-Defined Wide Area Network(SD-WAN)に関連する一般的な項目の知識があることが推奨されます。

使用するコンポーネント

このドキュメントの情報は、次のハードウェアに基づくものです。

- Cisco Catalyst SD-WAN Managerバージョン20.15.3
- Cisco IOS® XE Catalyst SD-WAN Edgesバージョン17.15.3a

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

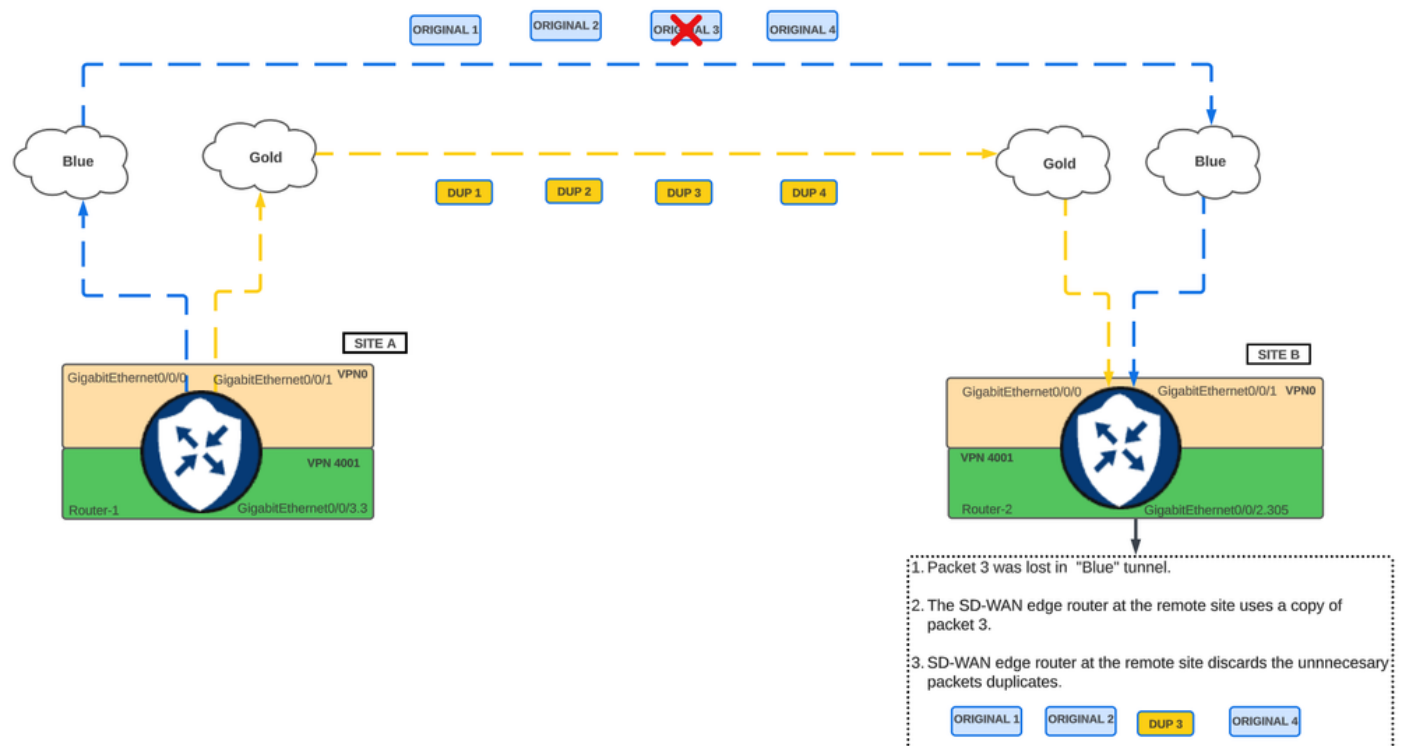
パケットの重複

パケット複製は、SD-WANエッジルータがネクストホップルータへの複数のオーバーレイIPsecトンネルを持つネットワークで、時間依存型アプリケーション(Voice over IP(VoIP)、ビデオ会議、金融取引、ミッションクリティカルな制御システムなど)の信頼性を確保し、パケット損失を削減するように設計されたSD-WAN機能です。

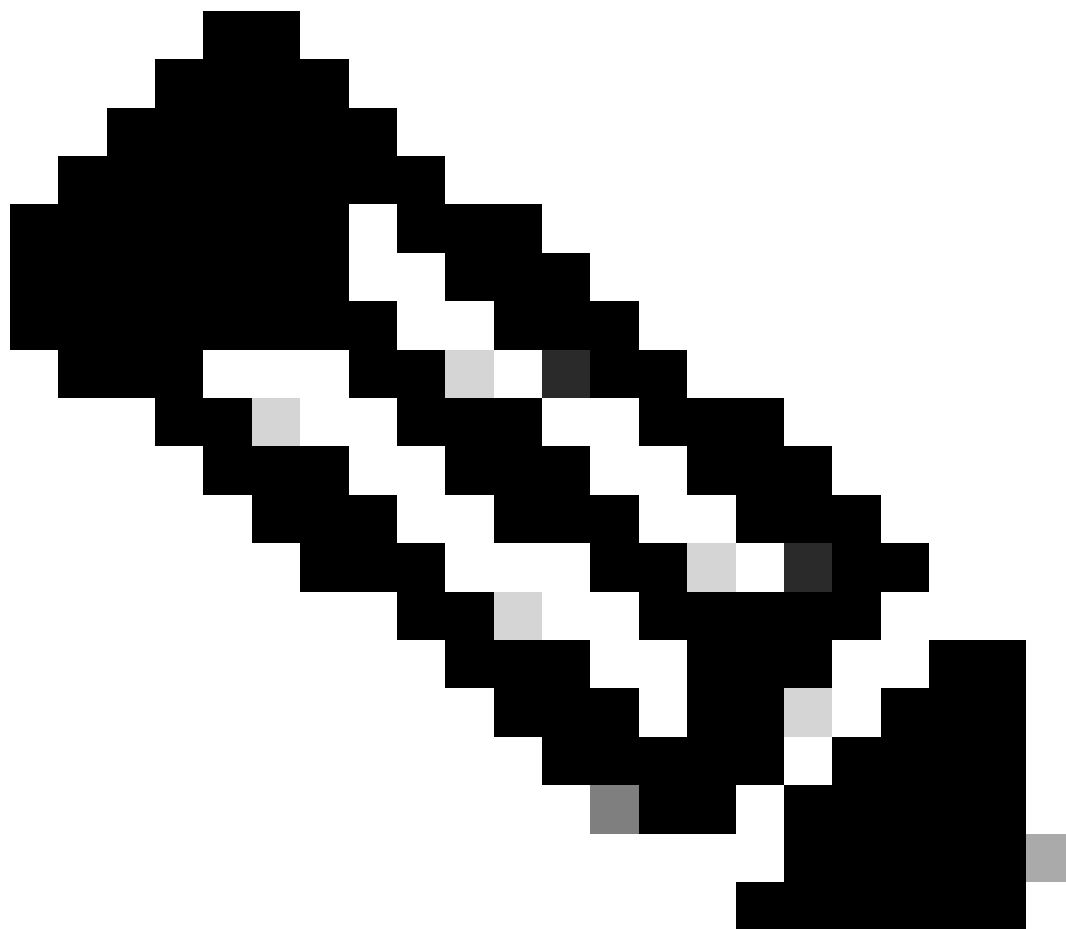
パケットの複製を有効にすると、SD-WANエッジルータは重複パケットを作成し、別のアクティブなIPsecトンネル経由でそれらを同時に送信します。

パケット複製のワークフロー

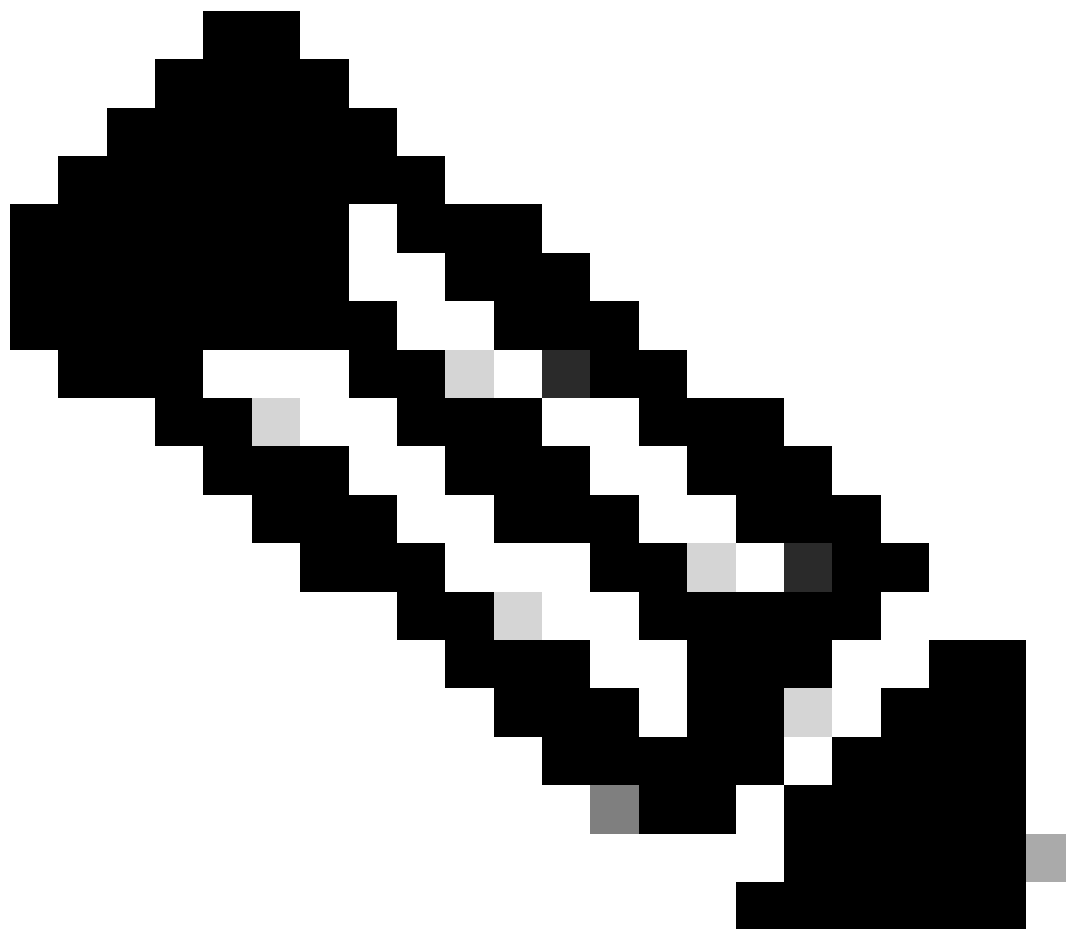
1. SD-WANエッジルータは、発信パケットの複製コピーを作成します。
2. 複製されたパケットは、別のトンネルIPsecトンネル経由で同時に送信されます。
3. 1つのパスでパケットが失われた場合、リモートサイトのSD-WANエッジルータは、別のトンネルで受信した同じパケットのコピーを処理します。
4. パケットが失われなければ、リモートサイトのSD-WANエッジルータは不要なパケットの複製を破棄します。



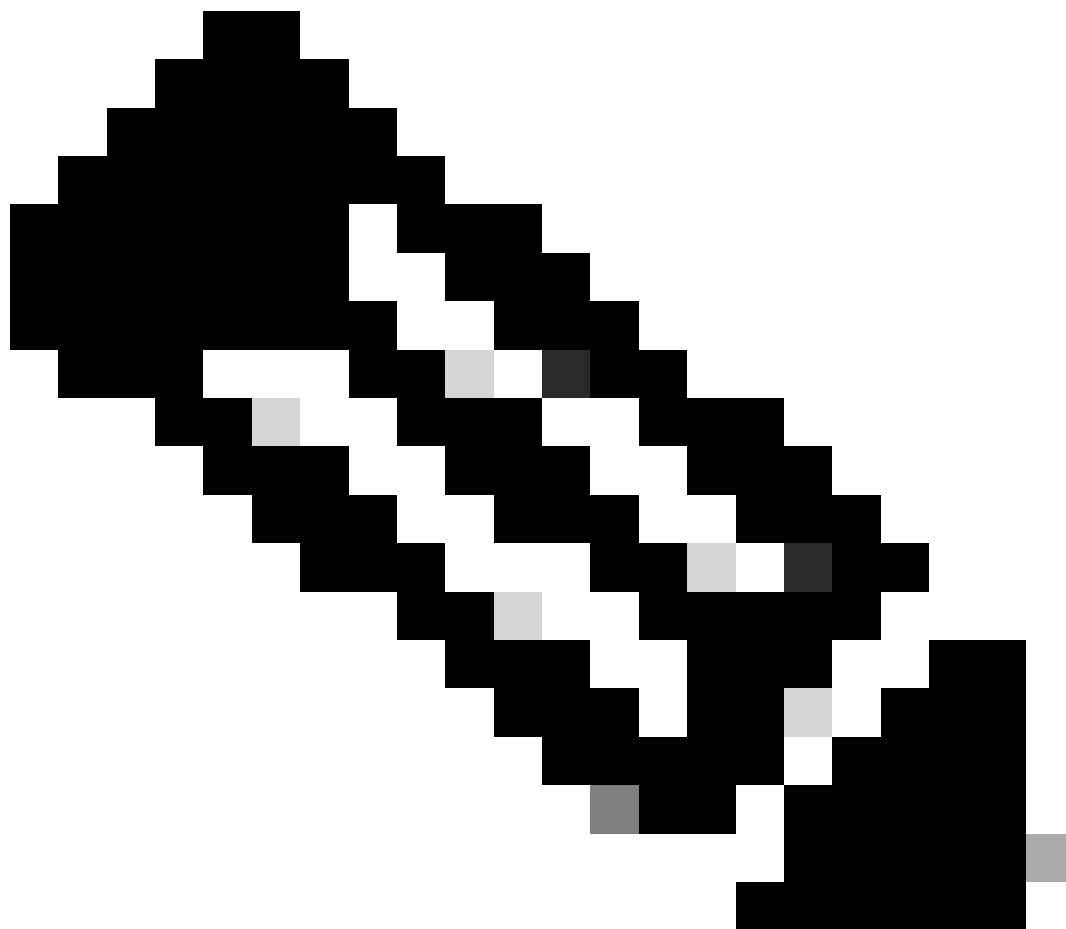
パケット複製のワークフロー



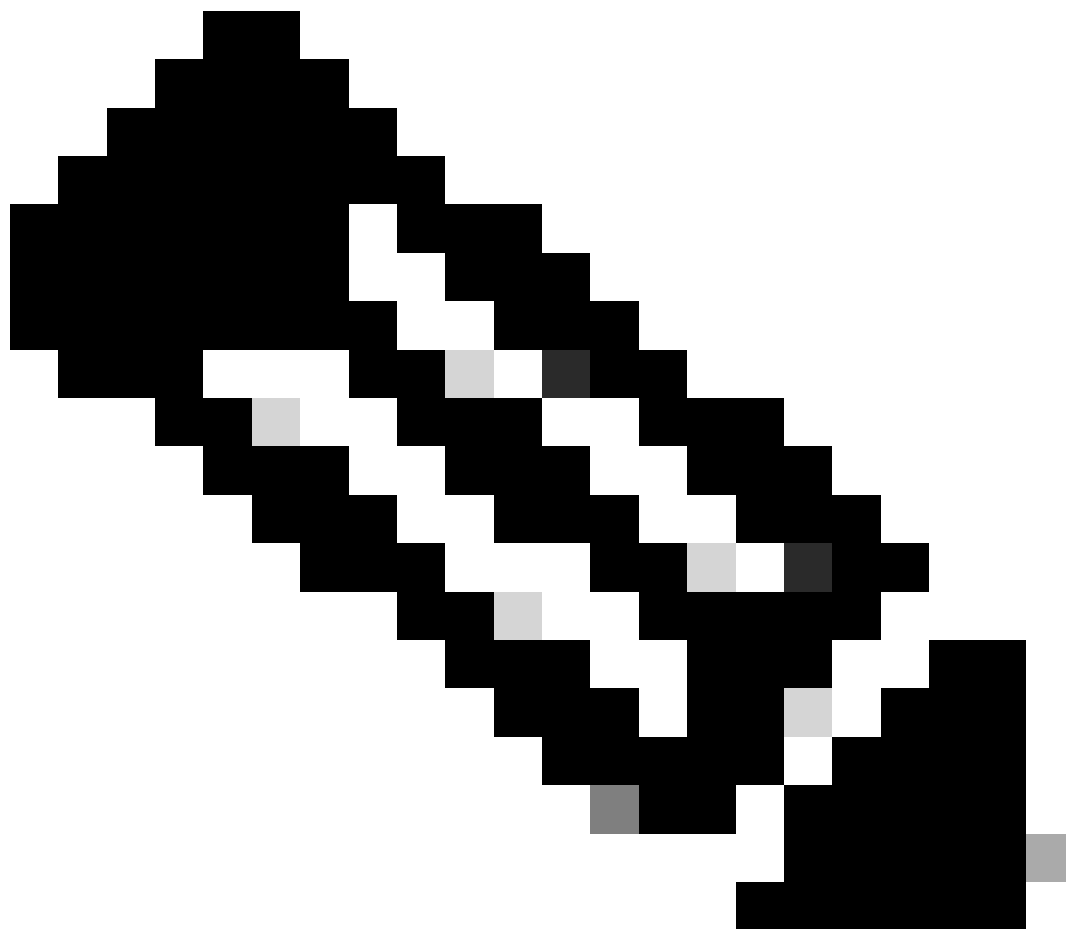
注：パケットの複製がサポートされているのは、SD-WANエッジルータがローカルサイトとリモートサイトの間に少なくとも2つのオーバーレイIPsecトンネルを確立するトポロジだけです。



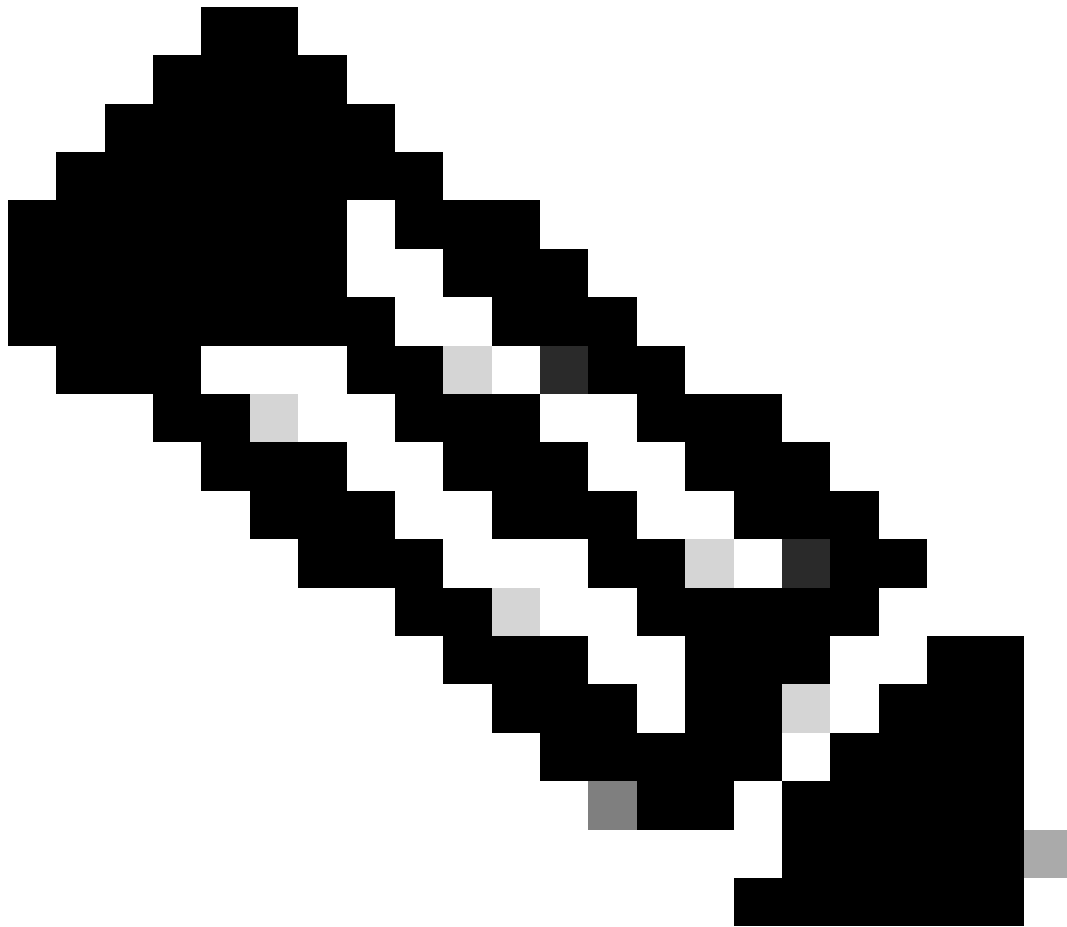
注：データポリシーおよびApplication-Aware Routing(AAR)は、パケット複製トラフィックには適用できません。



注: Cisco IOS XE Catalyst SD-WANデバイスでのパケット重複相互運用性、前方誤り訂正 (FEC)、およびTCP最適化は、Cisco IOS XEリリース16.xとCisco IOS XE Catalyst SD-WANリリース17.xのバージョンの間ではサポートされません。



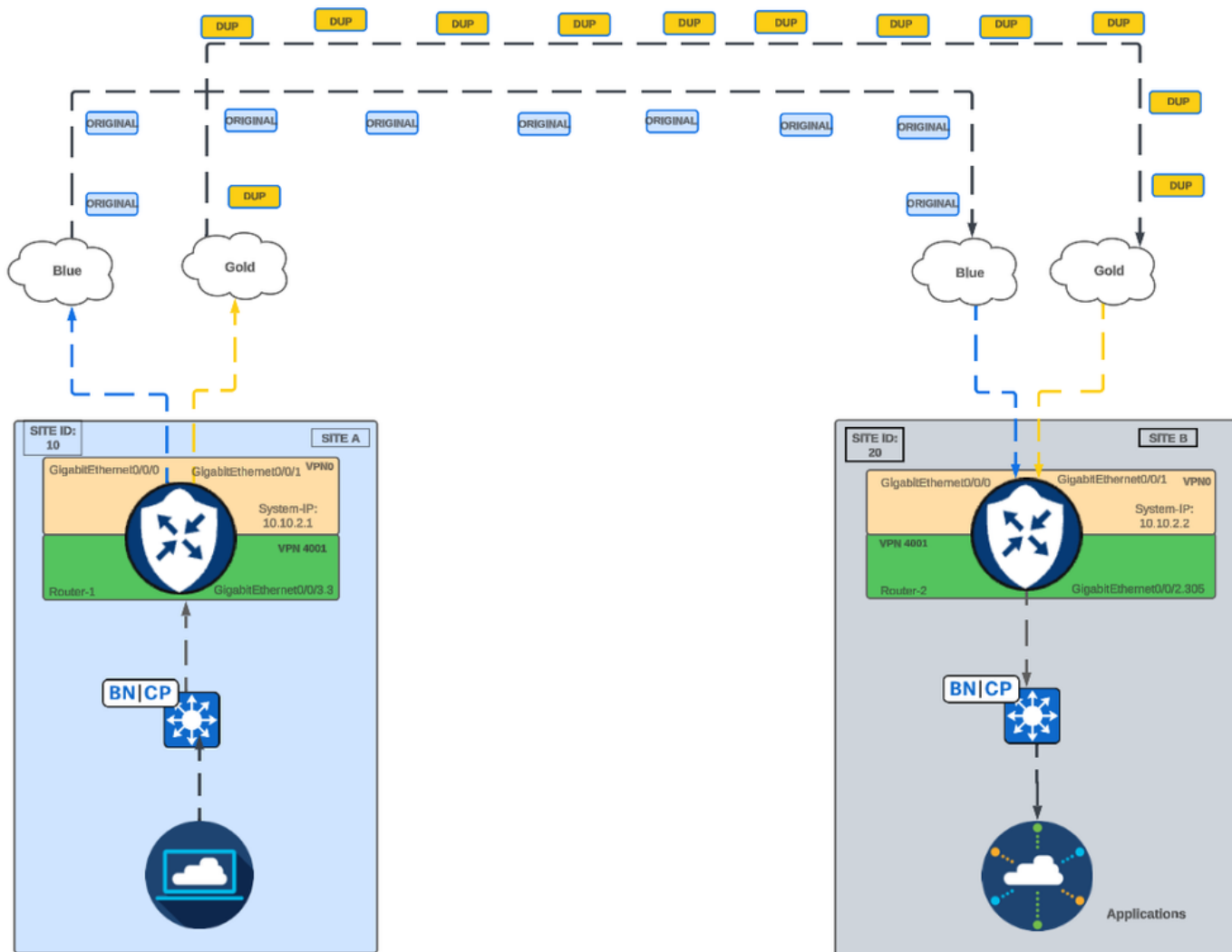
注：パケットの複製は、Cisco IOS XE Catalyst SD-WANデバイスでのみサポートされています。



注：パケットが代行受信されて複製されると、システムは着信トンネルIDを使用してIPデータベースを照会します。次に、重複するトンネルオブジェクトを取得します。システムは、パケット長と重複トンネルのパス最大伝送ユニット(PMTU)を比較します。パケット長が重複トンネルのPMTUより短い場合、パケットは重複します。

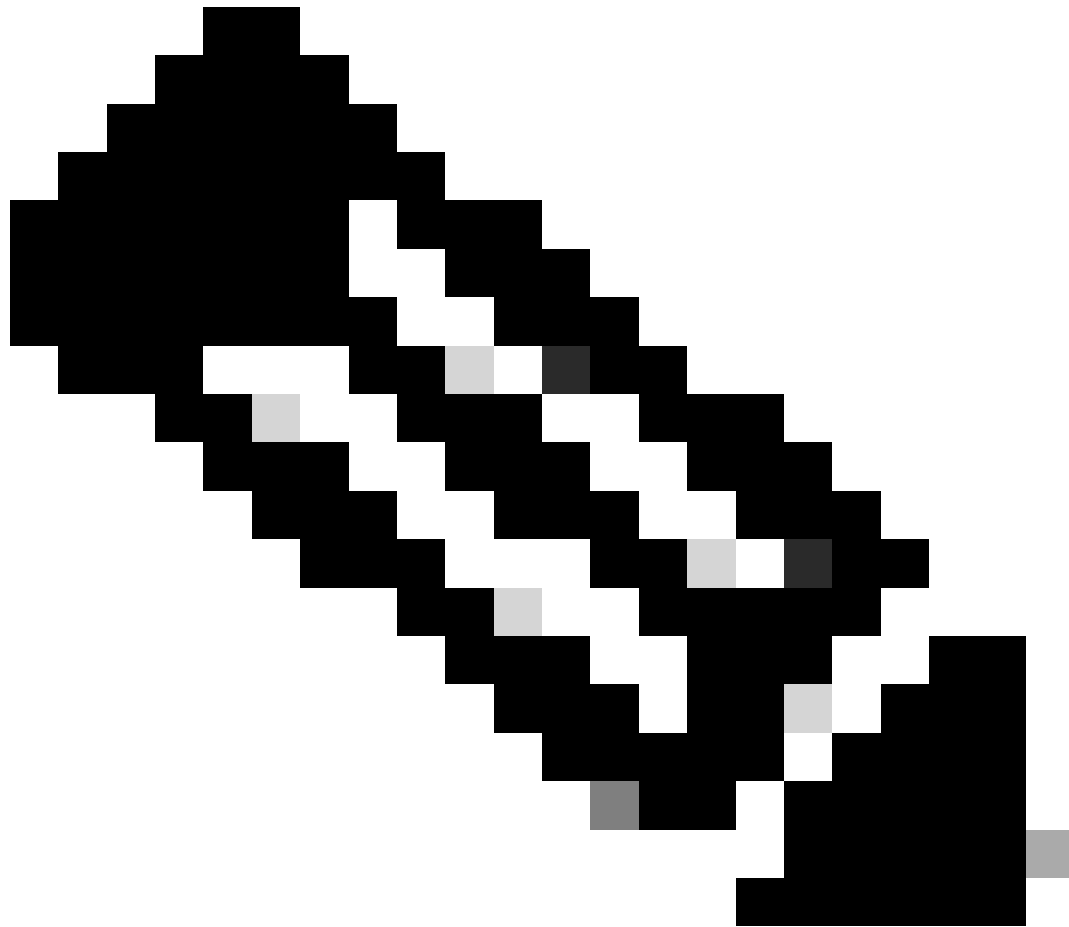
設定

ネットワーク図



サイト間ネットワーク図

ポリシーグループを使用したパケット複製の設定



注：サポートされる最小リリース：Cisco Catalyst SD-WANコントロールコンポーネント
リリース20.14.1

ステップ 1：アプリケーションの優先度とSLAポリシーの設定

- Cisco Catalyst SD-WAN ManagerのGUIにログインします。
- Configuration > Policy Groups > Application Priority & SLA > Add Application Priority & SLA Policyの順に移動します。
- Application Priority & SLA Policy nameを設定し、Createをクリックします。

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

アプリケーションの優先度とSLAポリシー名

- 右上のペインでAdvanced Layoutを有効にし、Add Traffic Policyをクリックします。

Cisco Catalyst SD-WAN

Policies > Application Priority & SLA

packet_duplication_tz

Additional Settings | Advanced Layout ☒

SLA Class | QoS Queue

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

+ Add Traffic Policy

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

高度なレイアウト

- Traffic PolicyName、service VPN(s) およびDirectionを設定します。
- デフォルトアクションの識別> Acceptの選択> Addのクリック

Add Traffic Policy List

Add Traffic Policy List

Policy Name
packet_duplication_tz_traffic_policy

VPN(s)
4001

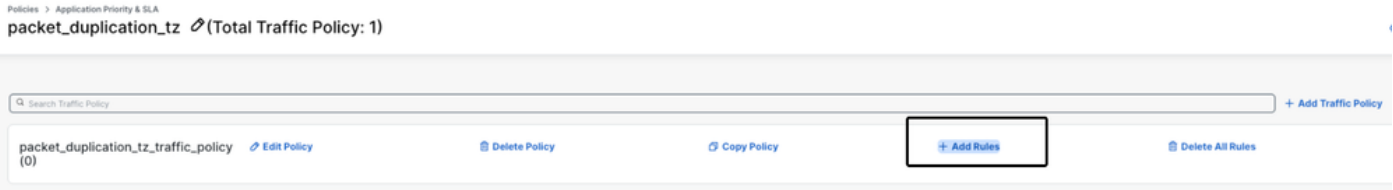
Direction
Service

Default Action
☒ Accept ☐ Drop

Cancel Add

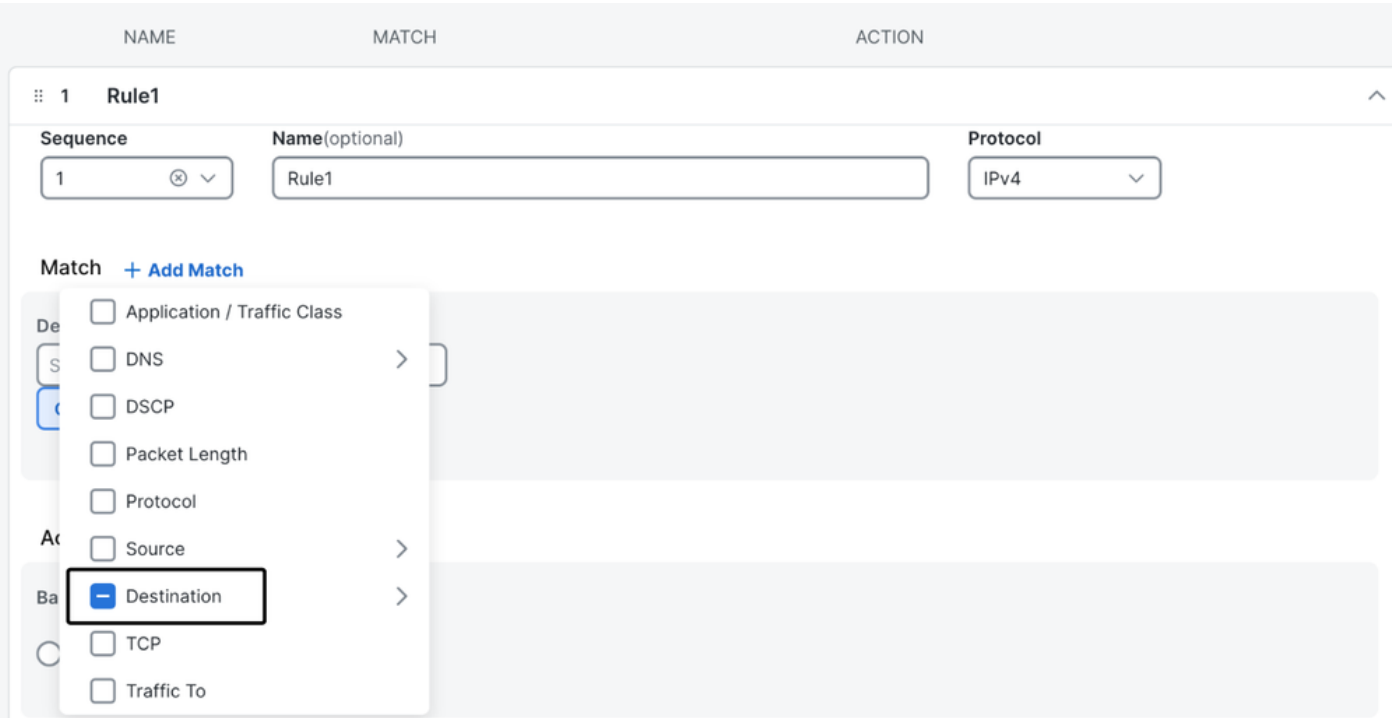
トラフィックポリシー名

- Add Rulesをクリックします。

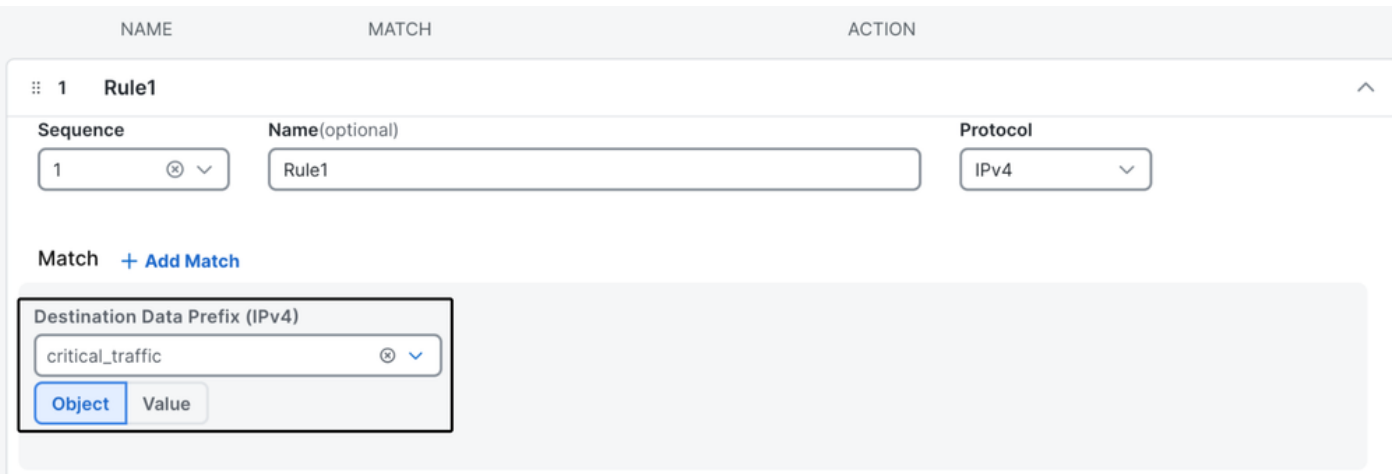


ルールの追加

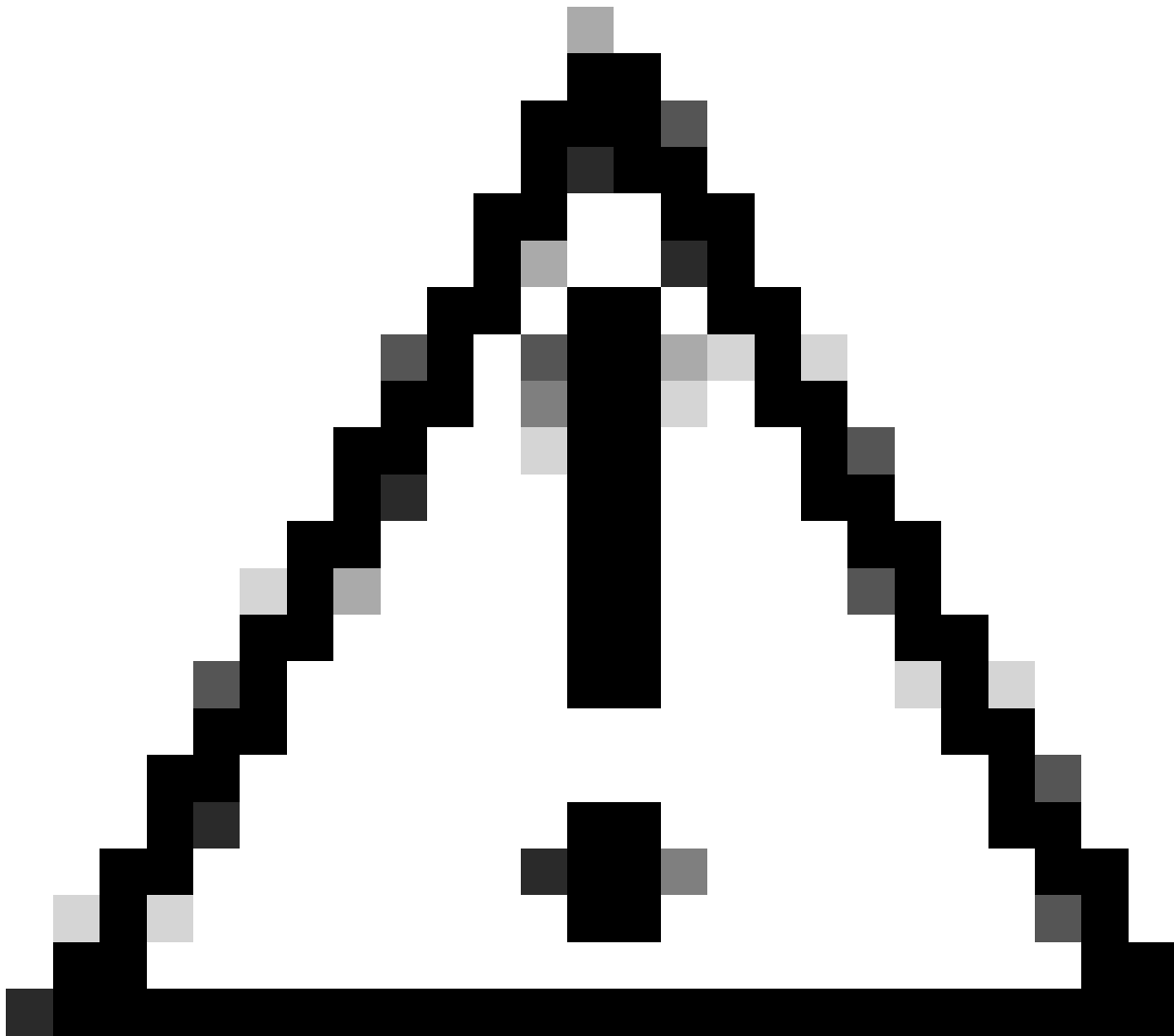
- Add Matchをクリックし、照合条件を選択します。



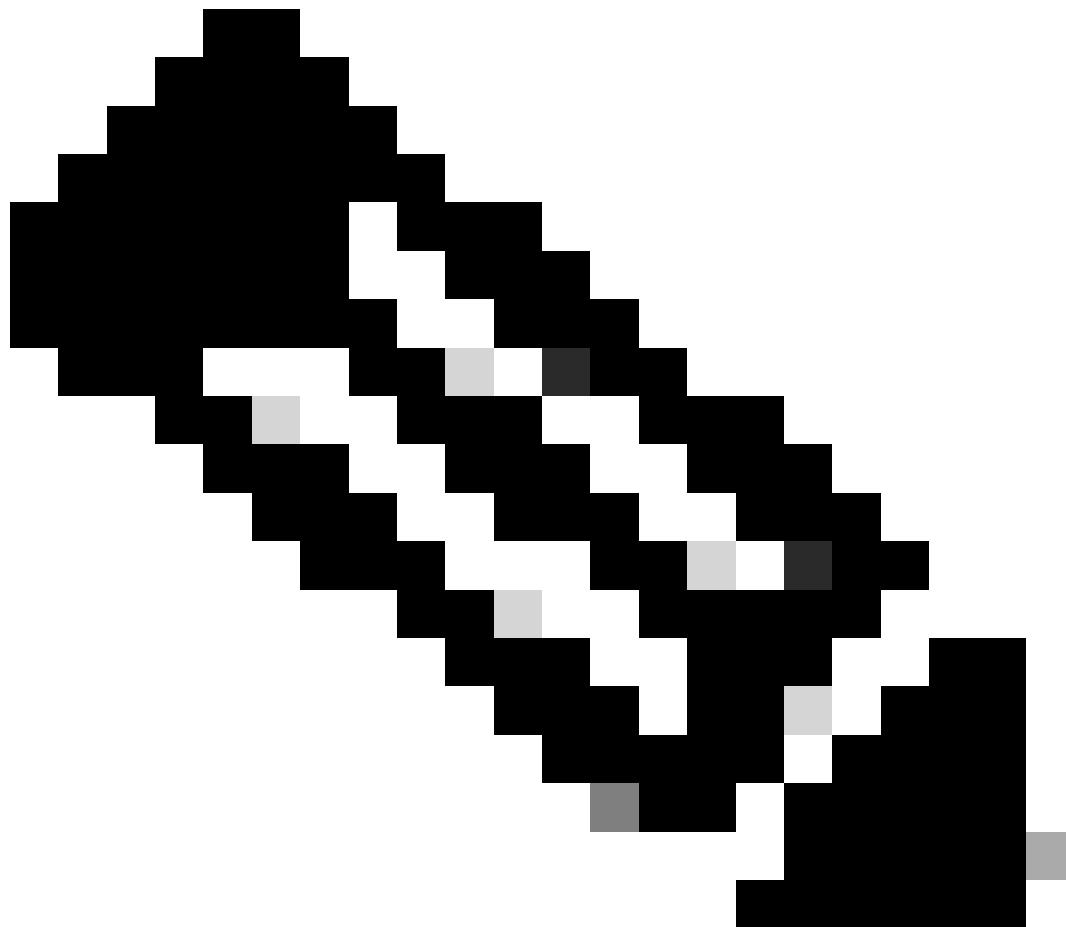
一致条件



宛先データプレフィックス



注意: SD-WANでのパケットの重複は、重要なアプリケーションまたは重要なトラフィックでの使用を目的としています。この機能をすべてのトラフィックタイプに対して有効にすることは推奨されません。有効にすると、SD-WANエッジルータのCPU負荷が増加し、パフォーマンスが低下する可能性があります。このラボテストの間、CPU使用率は約10 %増加しました。



注：このラボでは、照合条件として宛先データプレフィクスを使用します。また、Cisco Catalyst SD-WAN Managerは、必要に応じてアプリケーションまたはアプリケーションファミリリストの使用をサポートします。

-
- アクションの識別
 - Acceptを選択し、Add Action >Select Loss Correctionをクリックします。

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

アクションの追加

- Packet Duplicationを選択> Save Match and Actionsをクリック> Saveをクリック

Action [+ Add Action](#)

Base Action

☒ Accept ☐ Drop

Loss Correction

Type

Select one Type ^

FEC Adaptive

FEC Always

Packet Duplication

Cancel

Save Match and Actions

パケットの重複の選択

ステップ 2：ポリシーグループの定義

- Policy Groupに移動し、Add Policy Groupをクリックします。
- ポリシーグループ名とソリューションの設定>作成をクリックします

Add Policy Group

Policy Group Name

packet_duplication_policy_group_tz

Solution

sdwan

Description(optional)

Cancel

Create

ポリシーグループの定義

- アプリケーションの優先度の特定
- Application Priority & SLA Policy createdを選択> Saveをクリック

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

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							

アプリケーションの優先度とSLAポリシーの選択

- パケットの複製を有効にするSD-WANエッジルータを関連付けます。
- Associatedを識別し、Addをクリックします。
- Associated Devicesをクリック> Devicesを選択> Associated Devicesをクリック

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					

関連デバイス

Devices (0)

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
-----------------	-----------	----------	------	---------------	-----------	---------	---------------	---------------

デバイスの関連付け

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-cl	10.10.10.1	10	05328431376678528AE1	Yes

関連付けられるデバイス

- Provision Devicesをクリックし、Select Devices to Deployをクリックします。Deployをクリックします。

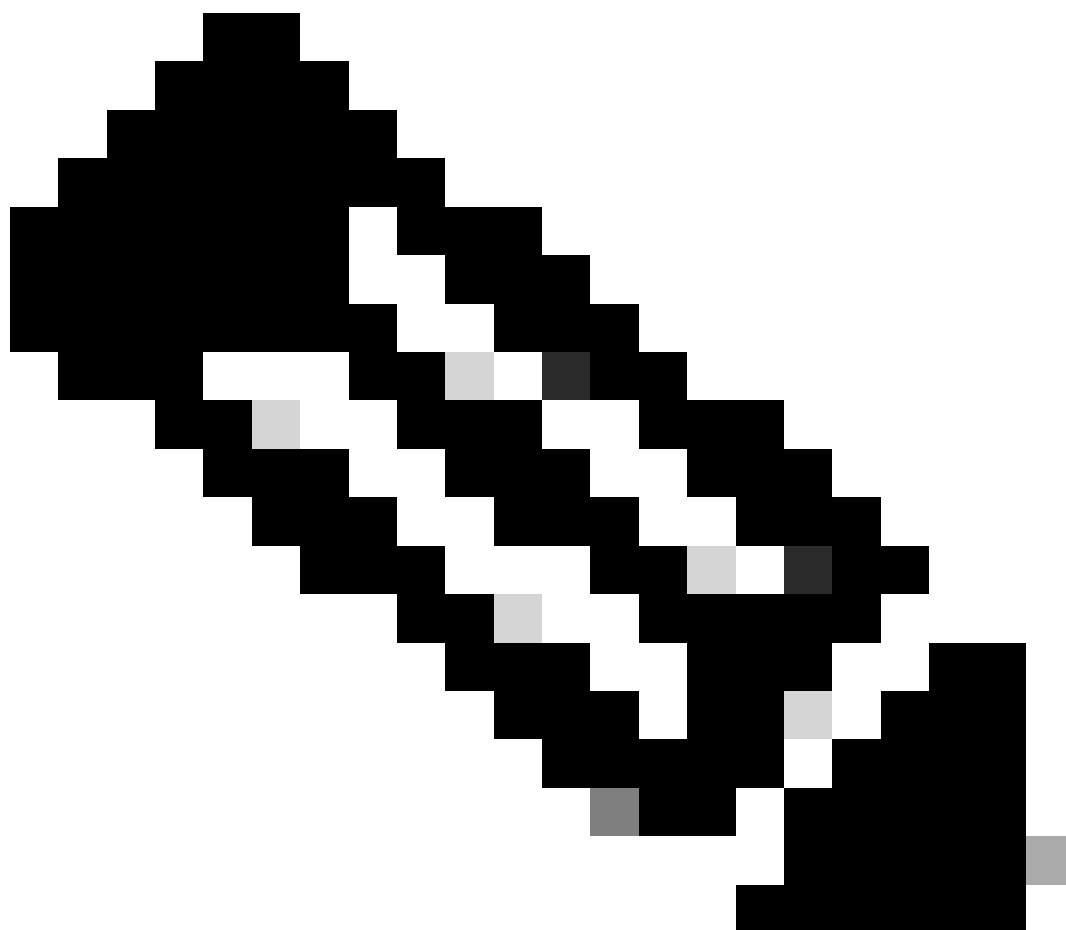
✔ **Do you want to provision devices in packet_duplication_policy_group_tz?**

Devices added to policy group packet_duplication_policy_group_tz!

No, I Will Do It Later

Provision Devices

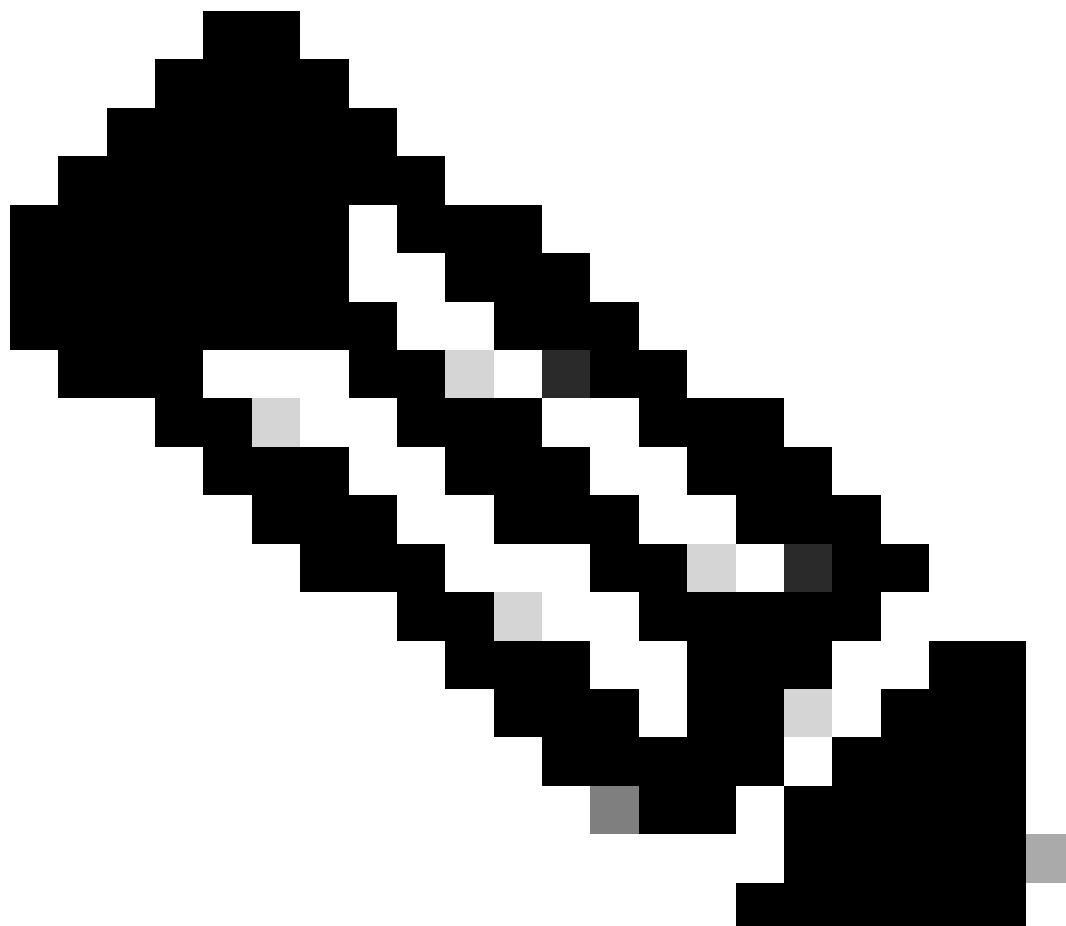
デバイスのプロビジョニング



注：ポリシーグループを導入する前に、設定グループをSD-WANエッジルータに関連付ける必要があります。

確認

SD-WANエッジルータのCLIからのパケット複製統計情報の監視



注: Cisco Catalyst SD-WANコントローラでパケットの重複を設定するためにSD-WANデータポリシーが使用され、設定はSD-WANエッジルータにプッシュされています。

show sdwan policy from-vsmartコマンドを実行して、Cisco Catalyst SD-WANコントローラからSD-WANエッジルータに送信されたデータポリシーを表示します。

```
<#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

show sdwan tunnel statistics pkt-dupコマンドを実行し、SD-WANトランスポートトンネルでのパケットの重複に関する統計情報を表示します。

<#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

show sdwan bfd sessions
コマンドを実行して、SD-WANエッジルータ間のBFDセッションのステータスと統計情報を表示します。

<#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

show platform hardware qfp active feature bfd datapath sdwan summary
コマンドを実行し、IPSEC SD-WANトンネルのハードウェア/データプレーンレベルでの統計情報を表示します。

<#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

show platform hardware qfp active feature sdwan client sysip summary コマンドを実行し、Quantum Flow Processor(QFP)で処理される、SD-WANクライアント機能に関連付けられたシステムIPアドレス(sysip)の要約を表示します。

TunID =プライマリローカルSD-WANトンネルのトンネルID (LDの末尾2桁に基づく)

DupID =セカンダリローカルSD-WANトンネルの複製ID (LDの末尾2桁に基づく)

<#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
-------	----	---	---	-------	-----	------

show platform hardware qfp active feature sdwan data sysip summary コマンドを実行し、データプレーンのSD-WANシステムIPの概要を表示します。

TunID =プライマリローカルSD-WANトンネルのトンネルID (LDの末尾2桁に基づく)

DupID =セカンダリローカルSD-WANトンネルの複製ID (LDの末尾2桁に基づく)

```
<#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  locCol  remCol  Encap  feC  mtu  sess-ppe
-----
77  0x6a9a4c60
10.10.2.2
      10      0x0      No      No      0
0
24

28

      20024  3      1      1      IPSEC      352      1442  0x6934f1a0
1
28

24

      20028  3      1      17      IPSEC      352      1442  0x6934f1e0
```

CPU使用率を確認するための追加コマンド：

```
<#root>

Router#

show processes cpu platform sorted | include CPU

Router##

show platform resources

Router#

show processes cpu history
```

Cisco Catalyst SD-WAN Managerからのパケット重複統計情報の監視

- Cisco SD-WAN Managerメニューから、Monitor > Devicesを選択します
- デバイスを選択します。
- デバイスの場合は、Action列で"..."をクリックし、Real Timeを選択します。
- Device Optionsドロップダウンメニューで、Tunnel Packet Duplication Statisticsを選択します。

Router | 10.10.10.1 Site Name SITE_10 Device Model: C8500-12X4QC ⓘ

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

パケット複製統計情報

関連情報

- [パケットの重複](#)
- [ポリシーグループ](#)
- [Cisco Catalyst SD-WANコンフィギュレーショングループ](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。