

Paketduplizierung mithilfe von Richtlinienengruppen im SD-WAN konfigurieren

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Paketduplizierung](#)

[Paketduplizierungs-Workflow](#)

[Wichtigste Punkte](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Paketduplizierung mithilfe von Richtlinienengruppen konfigurieren](#)

[Schritt 1: Konfigurieren der Anwendungspriorität und der SLA-Richtlinie](#)

[Schritt 2: Richtlinienengruppen definieren](#)

[Überprüfung](#)

[Überwachen von Paketduplizierungsstatistiken über die CLI des SD-WAN-Edge-Routers](#)

[Überwachen von Paketduplizierungsstatistiken über den Cisco Catalyst SD-WAN Manager](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird die Konfiguration der Paketduplizierung in Software-Defined Wide Area Networks (SD-WAN) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit allgemeinen Themen im Zusammenhang mit dem Cisco Catalyst Software-Defined Wide Area Network (SD-WAN) vertraut zu machen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

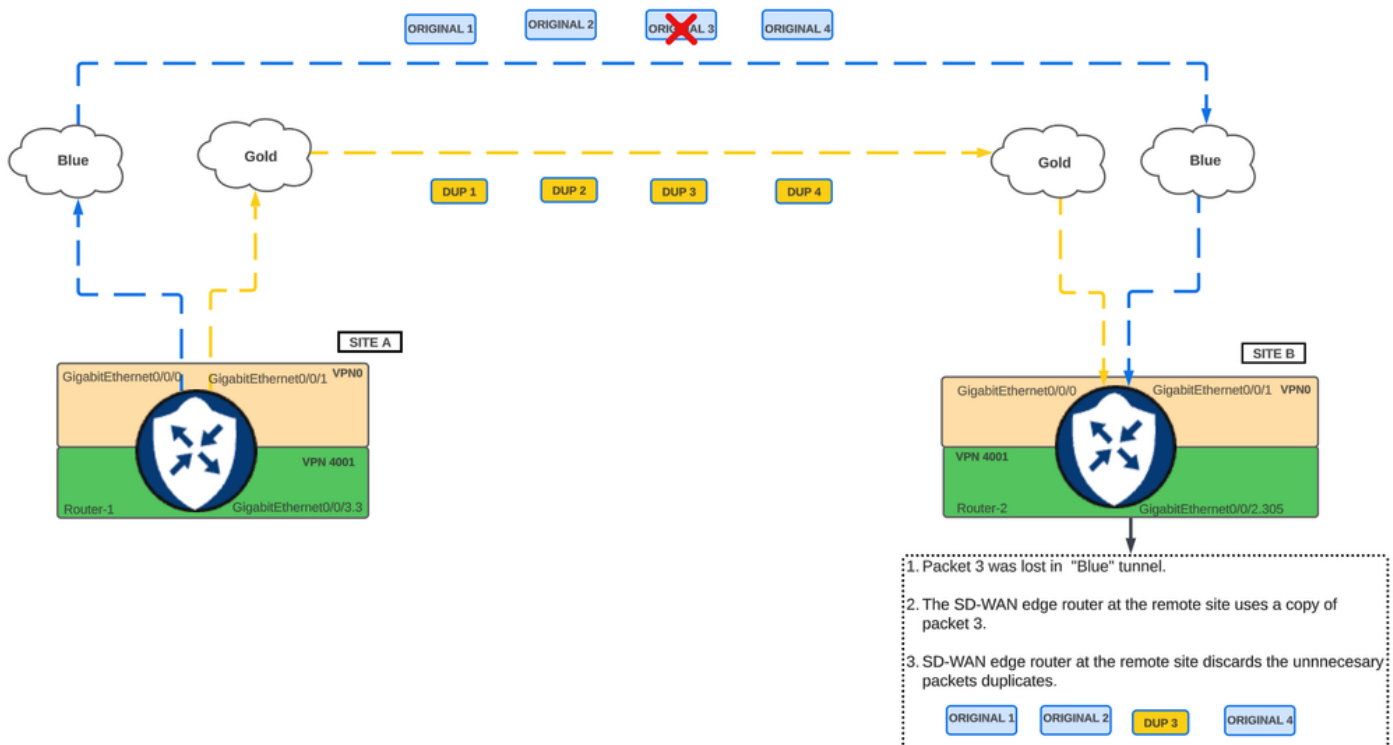
Paketduplizierung

Paketduplizierung ist eine SD-WAN-Funktion, die die Zuverlässigkeit sicherstellt und den Paketverlust für zeitkritische Anwendungen (wie Voice over IP (VoIP), Videokonferenzen, Finanztransaktionen und geschäftskritische Kontrollsysteme) in Netzwerken reduziert, in denen ein SD-WAN-Edge-Router über mehrere Overlay-IPsec-Tunnel zum Next-Hop-Router verfügt.

Bei aktivierter Paketduplizierung erstellt der SD-WAN-Edge-Router duplizierte Pakete und überträgt diese gleichzeitig über einen anderen aktiven IPsec-Tunnel.

Paketduplizierungs-Workflow

1. Der SD-WAN-Edge-Router erstellt doppelte Kopien des ausgehenden Pakets.
2. Die duplizierten Pakete werden gleichzeitig über einen anderen Tunnel-IPsec-Tunnel übertragen.
3. Wenn ein Paket über einen Pfad verloren geht, verarbeitet der SD-WAN-Edge-Router am Remote-Standort eine Kopie desselben Pakets, das über einen anderen Tunnel empfangen wurde.
4. Wenn keine Pakete verloren gehen, verwirft der SD-WAN-Edge-Router am Remote-Standort die unnötigen Paketduplikate.

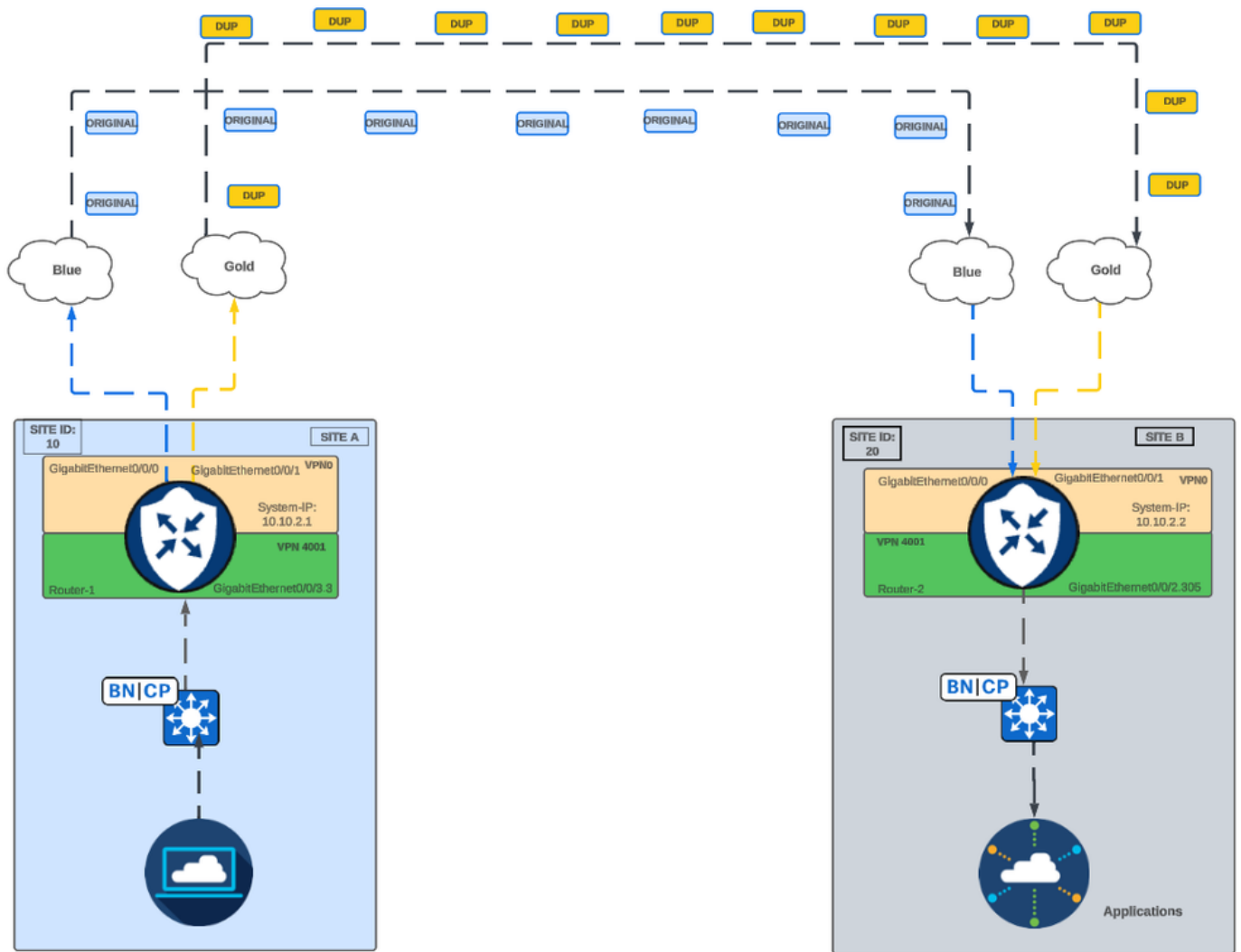


Wichtigste Punkte

- Paketduplizierung wird nur in Topologien unterstützt, in denen SD-WAN-Edge-Router mindestens zwei IPsec-Overlay-Tunnel zwischen dem lokalen Standort und dem Remote-Standort einrichten.
- Datenrichtlinien und anwendungssensitives Routing (AAR) dürfen nicht auf paketduplizierten Datenverkehr angewendet werden.
- Die Versionen Cisco IOS XE 16.x und Cisco IOS XE Catalyst SD-WAN 17.x unterstützen keine Paketduplizierungs-Interop, Vorwärtsfehlerkorrektur (FEC) und TCP-Optimierung auf Cisco IOS XE Catalyst SD-WAN-Geräten.
- Die Paketduplizierung wird nur auf Cisco IOS XE Catalyst SD-WAN-Geräten unterstützt.
- Wenn Pakete zur Duplizierung abgefangen werden, fragt das System die IP-Datenbank unter Verwendung der eingehenden Tunnel-ID ab. Anschließend wird das doppelte Tunnelobjekt abgerufen. Das System vergleicht die Paketlänge mit der Path Maximum Transmission Unit (PMTU) des duplizierten Tunnels. Wenn die Paketlänge kleiner ist als die PMTU des duplizierten Tunnels, werden die Pakete dupliziert.

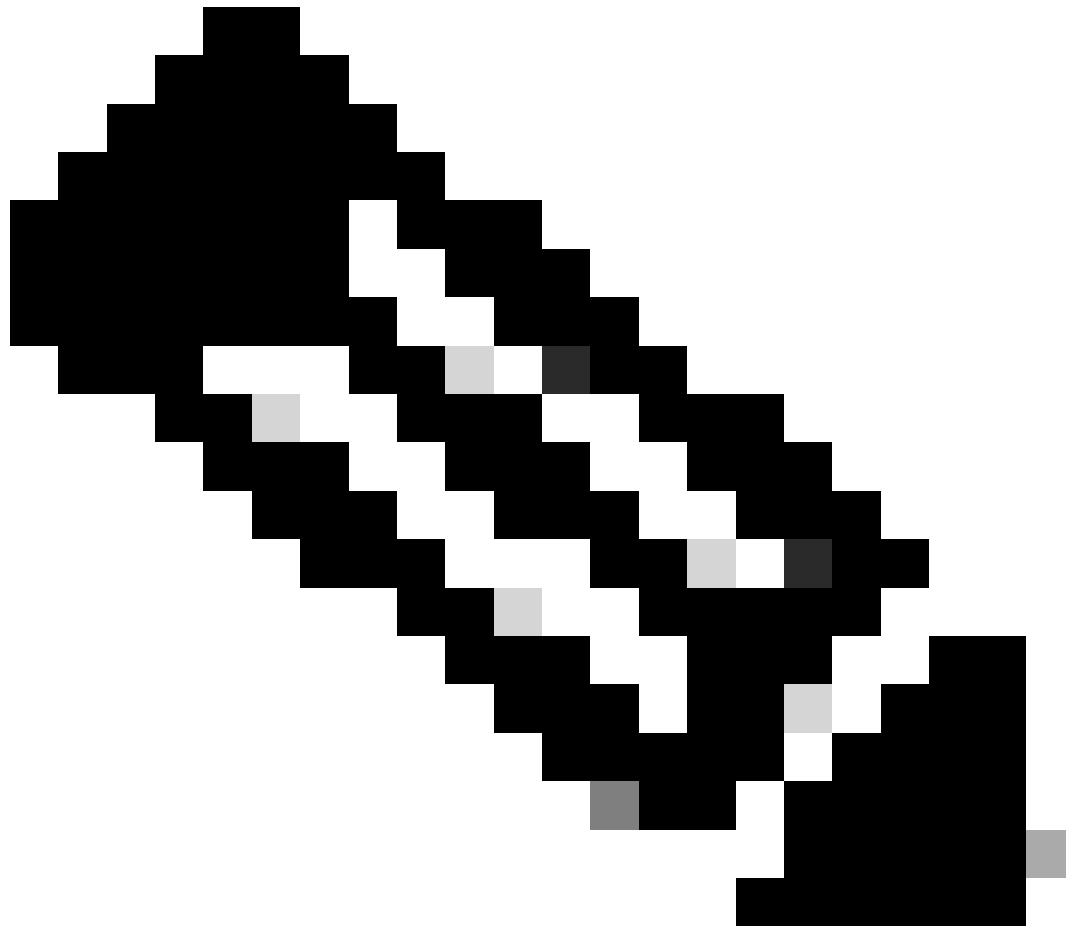
Konfigurieren

Netzwerkdiagramm



Site-to-Site-Netzwerkdigramm

Paketduplizierung mithilfe von Richtliniengruppen konfigurieren



Anmerkung: Unterstützte Mindestversion: Cisco Catalyst SD-WAN Control Components Version 20.14.1

Schritt 1: Konfigurieren der Anwendungspriorität und der SLA-Richtlinie

- Melden Sie sich bei der Cisco Catalyst SD-WAN Manager-GUI an.
- Navigieren Sie zu Konfiguration > Richtliniengruppen > Anwendungspriorität und SLA > Anwendungspriorität und SLA-Richtlinie hinzufügen.
- Konfigurieren Sie die Anwendungspriorität und den SLA-Richtliniennamen. > Klicken Sie auf "Erstellen".

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

Name der Anwendungspriorität und der SLA-Richtlinie

- Aktivieren Sie Erweitertes Layout im rechten oberen Bereich > klicken Sie auf Datenverkehrsrichtlinie hinzufügen.

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

Layout erweitern

- Konfigurieren Sie Traffic PolicyName, Service-VPN(s) und Richtung.
- Standardaktion identifizieren > Akzeptieren auswählen > auf Hinzufügen klicken

Add Traffic Policy List

Add Traffic Policy List

Policy Name
packet_duplication_tz_traffic_policy

VPN(s)
4001

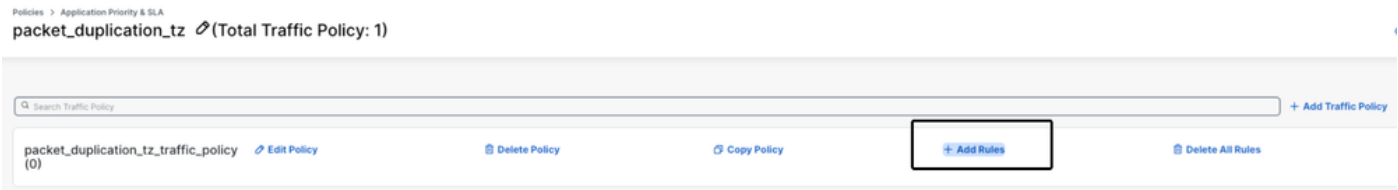
Direction
Service

Default Action
☒ Accept ☐ Drop

Cancel Add

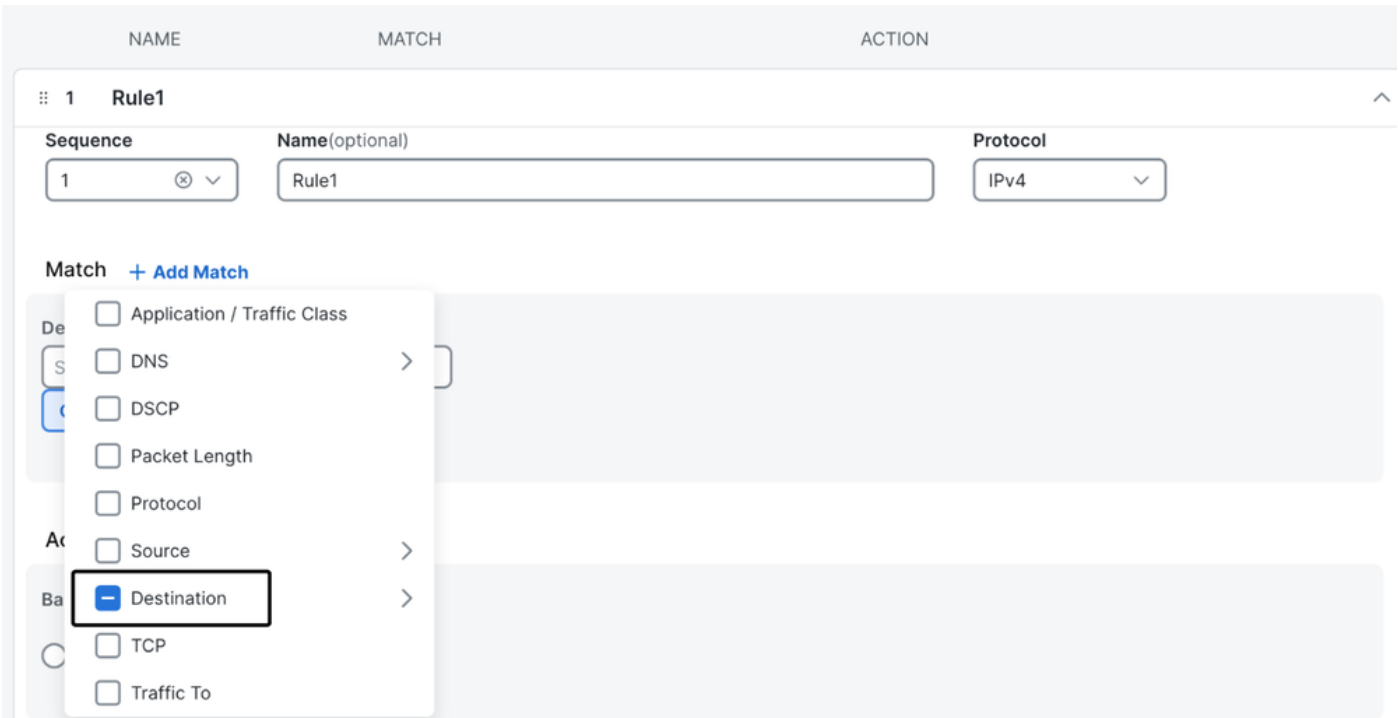
Name der Datenverkehrsrichtlinie

- Klicken Sie auf Regeln hinzufügen.

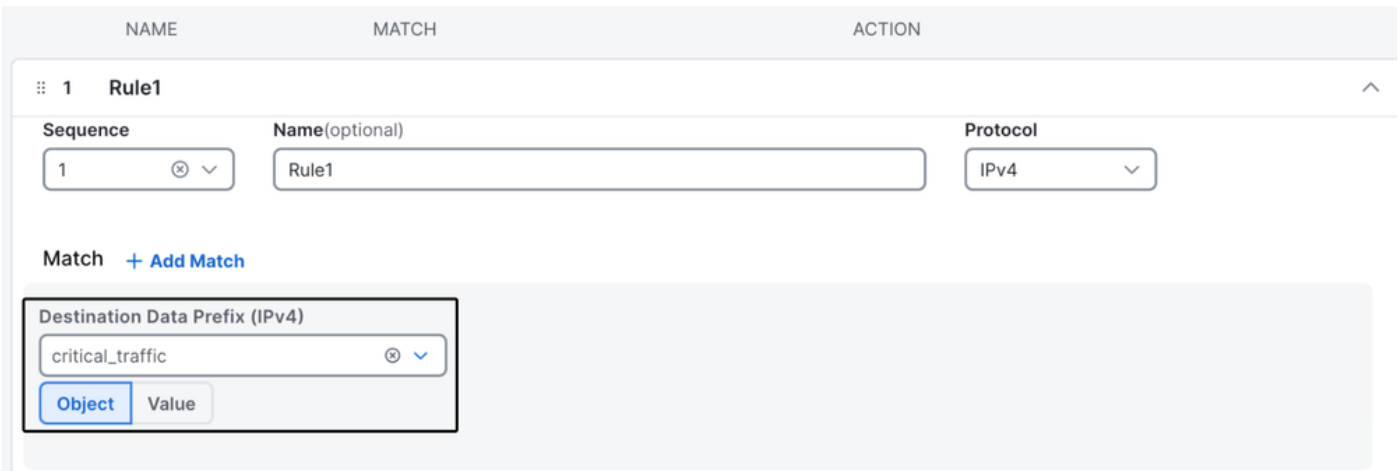


Regeln hinzufügen

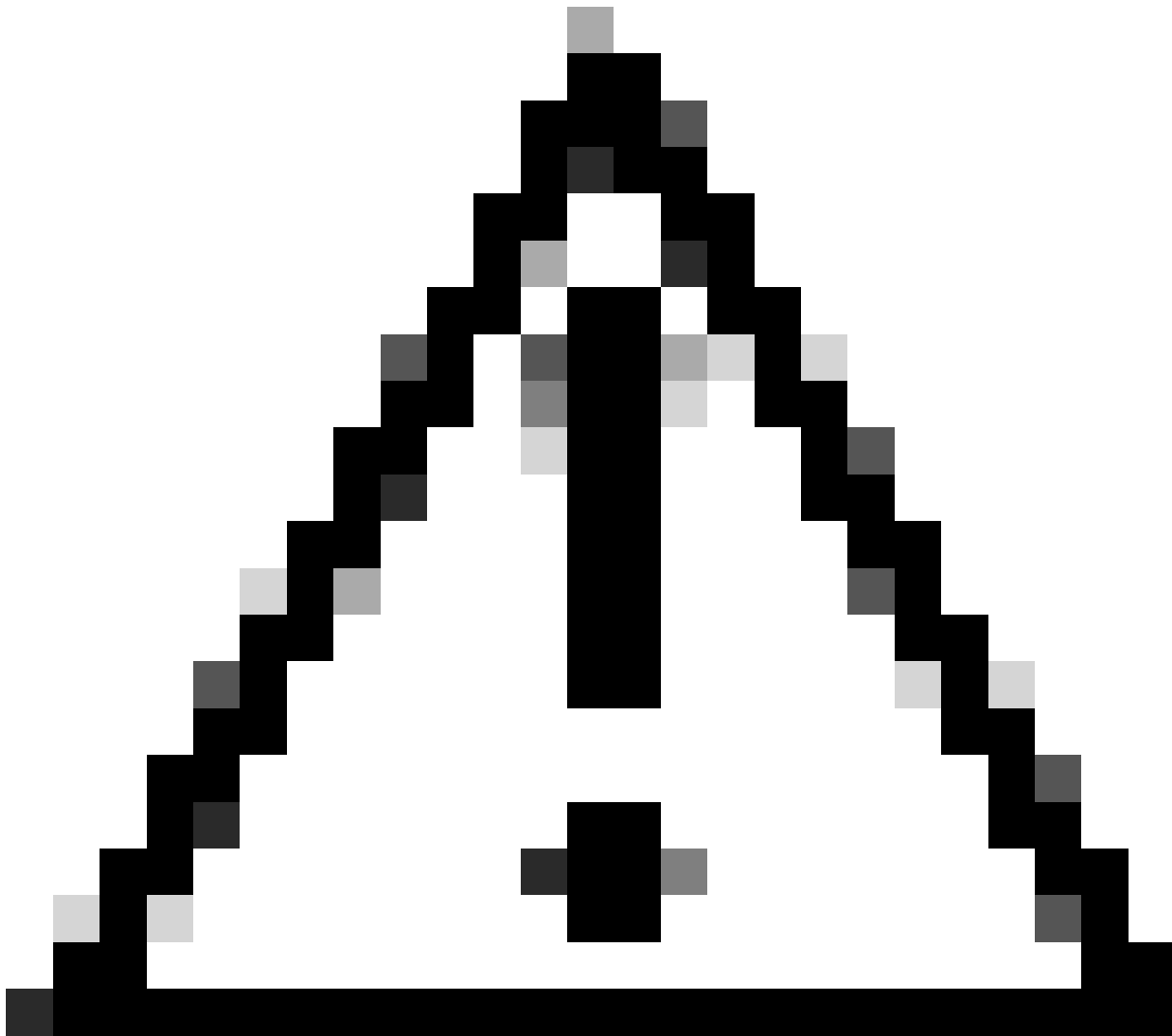
- Klicken Sie auf Übereinstimmung hinzufügen > Übereinstimmungsbedingung auswählen.



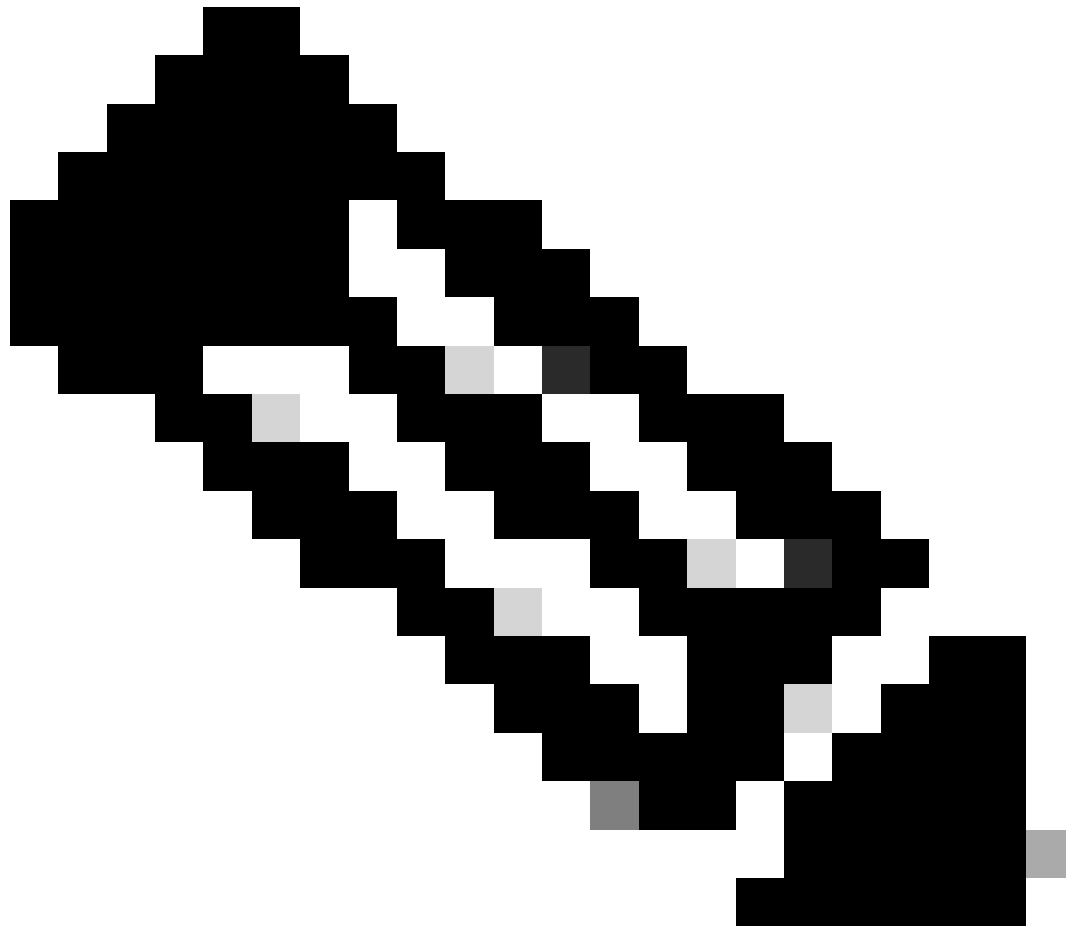
Übereinstimmungsbedingungen



Präfix für Zieldaten



Vorsicht: Die Paketduplizierung im SD-WAN ist für die Verwendung mit kritischen Anwendungen oder kritischem Datenverkehr vorgesehen. Die Aktivierung dieser Funktion für alle Datenverkehrstypen wird nicht empfohlen, da sie zu einer höheren CPU-Auslastung und einer potenziellen Leistungsminderung auf dem SD-WAN-Edge-Router führt. Während dieses Labortests stieg die CPU-Auslastung um ca. 10 %.



Anmerkung: Dieses Labor verwendet das Präfix für Zieldaten als Übereinstimmungsbedingung. Darüber hinaus unterstützt der Cisco Catalyst SD-WAN Manager bei Bedarf die Verwendung von Anwendungen oder Anwendungsfamilienlisten.

-
- Aktion identifizieren
 - Wählen Sie Akzeptieren > klicken Sie auf Aktion hinzufügen > Wählen Sie Verlustkorrektur

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

Aktion hinzufügen

- Wählen Sie Paketduplizierung aus > klicken Sie auf Übereinstimmung speichern und Aktionen > klicken Sie auf Speichern.

Action [+ Add Action](#)

Base Action

☒ Accept ☐ Drop

Loss Correction

Type

Select one Type ^

FEC Adaptive

FEC Always

Packet Duplication

Cancel

Save Match and Actions

Paketduplizierung auswählen

Schritt 2: Richtliniengruppen definieren

- Navigieren Sie zu Policy Group > Klicken Sie auf Add Policy Group.
- Konfigurieren von Richtliniengruppen-Name und -Lösung > Klicken Sie auf "Erstellen"

Add Policy Group

Policy Group Name

packet_duplication_policy_group_tz

Solution

sdwan

Description(optional)

Cancel

Create

Definieren von Richtliniengruppen

- Identifizieren der Anwendungspriorität
- Wählen Sie Anwendungspriorität und erstellte SLA-Richtlinie aus > klicken Sie auf Speichern.

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

Application Priority

Please Select one

packet_duplication_tz

Create New

Description(optional)

NGFW
Please Select one

DNS Security
Please Select one

Device Solution
Type sdwan
Deployment
Associated + Add
Save Deploy

Auswahl von Anwendungspriorität und SLA-Richtlinie

- Verknüpfen Sie die SD-WAN-Edge-Router, auf denen die Paketduplizierung aktiviert werden soll.
- Zugeordnet identifizieren > Klicken Sie auf Hinzufügen.
- Klicken Sie auf Associated Devices > Choose Devices (Geräte auswählen) > Click on Associated Devices (Zugeordnete Geräte auswählen)

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

Application Priority

Secure Internet Gateway / Secure Service Edge
Please Select one

Description(optional)

NGFW
Please Select one

DNS Security
Please Select one

Device Solution
Type sdwan
Deployment
Associated + Add
Save Deploy

Zugeordnete Geräte

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

Zuordnen - Geräte

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-cls	10.10.10.1	10	05328431376678528AE1	Yes
Items per page: 25 1 - 1 of 1 < < > >							

Zuzuordnende Geräte

- Klicken Sie auf Provisioning Devices > Select Devices to Deploy > Click on Deploy.

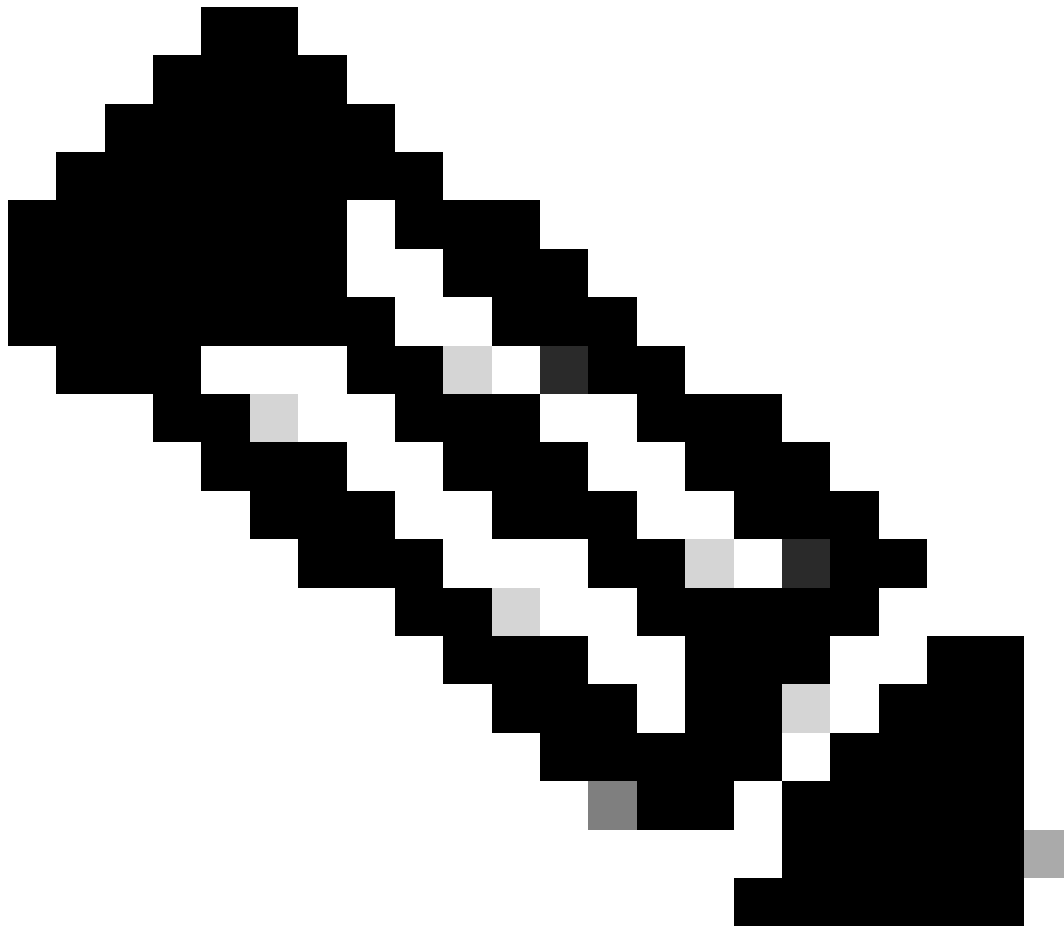
✔ **Do you want to provision devices in packet_duplication_policy_group_tz?**

Devices added to policy group packet_duplication_policy_group_tz!

No, I Will Do It Later

Provision Devices

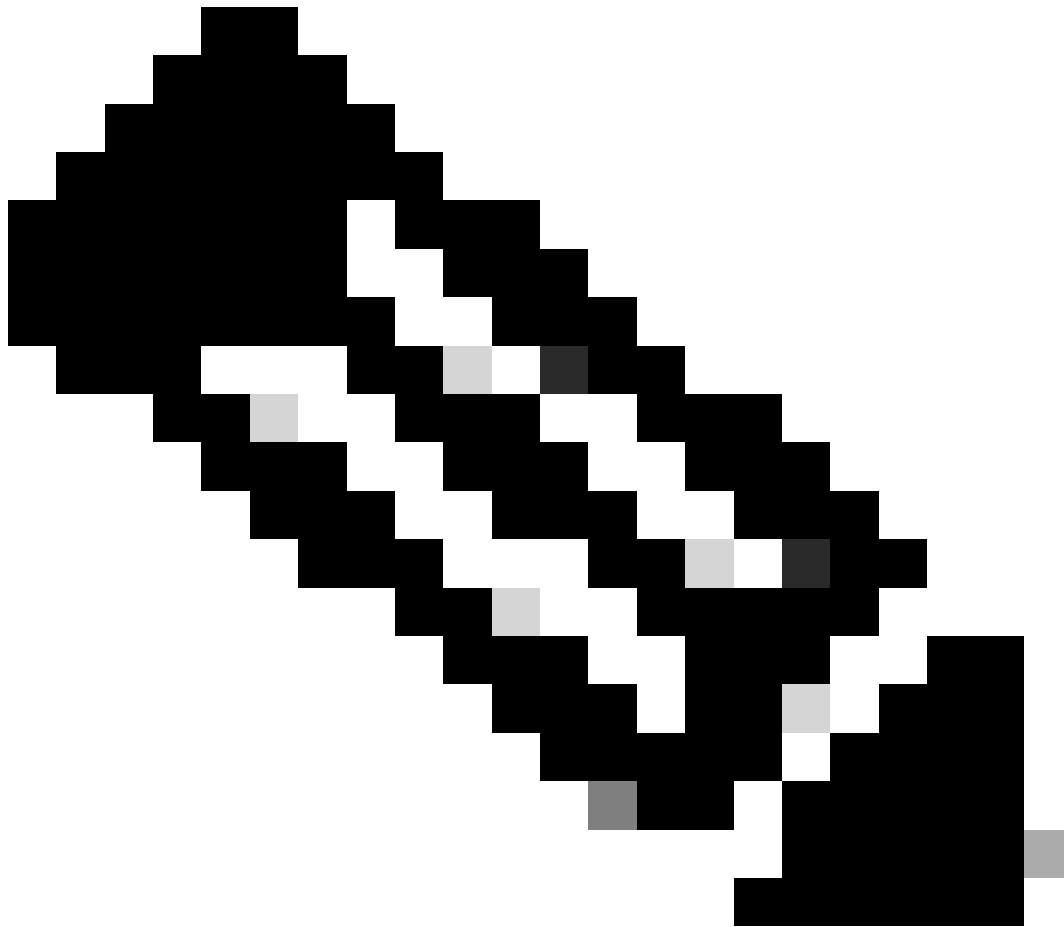
Bereitstellung von Geräten



Anmerkung: Vor der Bereitstellung einer Richtliniengruppe muss eine Konfigurationsgruppe mit dem SD-WAN-Edge-Router verknüpft werden.

Überprüfung

Überwachen von Paketduplizierungsstatistiken über die CLI des SD-WAN-Edge-Routers



Anmerkung: Mit einer SD-WAN-Datenrichtlinie wurde die Paketduplizierung auf dem Cisco Catalyst SD-WAN-Controller konfiguriert, und die Konfiguration wurde per Push an den SD-WAN-Edge-Router übertragen.

Führen Sie den Befehl `show sdwan policy from-vsmart` aus, um die Datenrichtlinien anzuzeigen, die vom Cisco Catalyst SD-WAN-Controller an den SD-WAN-Edge-Router gesendet wurden.

```
<#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
```

Führen Sie den Befehl `show sdwan tunnel statistics pkt-dup` aus, um Statistiken zur Paketduplizierung in SD-WAN-Transporttunneln anzuzeigen.

<#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

Führen Sie den Befehl `show sdwan bfd sessions` aus, um den Status und die Statistiken der BFD-Sitzungen zwischen SD-WAN-Edge-Routern anzuzeigen.

<#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

Führen Sie den Befehl `show platform hardware qfp active feature bfd datapath sdwan summary` aus, um die Statistiken auf Hardware-/Datenebene für IPSEC-SD-WAN-Tunnel anzuzeigen.

<#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

Führen Sie den Befehl `show platform hardware qfp active feature sdwan client sysip summary` aus, um eine Zusammenfassung der System-IP-Adressen (sysip) anzuzeigen, die der SD-WAN-Client-Funktion zugeordnet sind, wie sie vom Quantum Flow Processor (QFP) verarbeitet wurde.

TunID = Tunnel-ID des primären lokalen SD-WAN-Tunnels (basierend auf den letzten 2 Ziffern der LD)

DupID = TheDuplikations-ID des sekundären lokalen SD-WAN-Tunnels (basierend auf den letzten 2 Stellen der 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
-------	----	---	---	-------	-----	------

Führen Sie den Befehl `show platform hardware qfp active feature sdwan data sysip summary` aus, um eine Zusammenfassung der SD-WAN-System-IPs auf der Datenebene anzuzeigen.

TunID = Tunnel-ID des primären lokalen SD-WAN-Tunnels (basierend auf den letzten 2 Ziffern der LD)

DupID = TheDuplikations-ID des sekundären lokalen SD-WAN-Tunnels (basierend auf den letzten 2 Stellen der LD)

<#root>

Router#

show platform hardware qfp active feature sdwan data sysip summary

BktIdx Idx	BktAddr	SysIP	SiteID	Next	on-demnd	Gleaning	glean_ipc_paks
---------------	---------	-------	--------	------	----------	----------	----------------

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

Zusätzliche Befehle zur Überprüfung der CPU-Auslastung:

<#root>

Router#

show processes cpu platform sorted | include CPU

Router##

show platform resources

Router#

show processes cpu history

Überwachen von Paketduplizierungsstatistiken vom Cisco Catalyst SD-WAN Manager

- Wählen Sie im Menü Cisco SD-WAN Manager die Option Monitor > Devices (Überwachung > Geräte).
- Wählen Sie ein Gerät.
- Klicken Sie für ein Gerät in der Spalte Aktion auf "...". und wähle "Echtzeit".
- Wählen Sie im Dropdown-Menü Device Options (Geräteoptionen) die Option Tunnel Packet Duplication Statistics (Tunnelpaketduplizierungsstatistik).

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

Device Options:

Q 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

Paketduplizierungsstatistik

Zugehörige Informationen

- [Paketduplizierung](#)
- [Richtliniengruppen](#)
- [Cisco Catalyst SD-WAN-Konfigurationsgruppen](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.