

# Konfigurieren und Überprüfen von DIA NAT Tracker und Fallback

## Inhalt

---

### [Einleitung](#)

### [Voraussetzungen](#)

#### [Anforderungen](#)

#### [Verwendete Komponenten](#)

#### [Einschränkungen für NAT DIA Tracker](#)

[Einschränkungen für Cisco IOS XE Catalyst SD-WAN Version 17.10.1a und frühere Versionen](#)

[Einschränkungen für Cisco IOS XE Catalyst SD-WAN Version 17.11.1a](#)

[Einschränkungen für Cisco IOS XE Catalyst SD-WAN Version 17.13.1a](#)

#### [Unterstützte Schnittstellen für NAT DIA Tracker](#)

### [Konfigurieren](#)

#### [Netzwerkdiagramm](#)

#### [Konfigurationen](#)

#### [Schritt 1: NAT DIA Tracker konfigurieren](#)

#### [Schritt 2: Anbinden des Trackers an die Transportschnittstelle](#)

#### [Schritt 3: NAT-Fallback für vorhandene DIA-Richtlinie aktivieren](#)

### [Überprüfung](#)

### [Tracker zur Fehlerbehebung](#)

### [Zugehörige Informationen](#)

---

## Einleitung

In diesem Dokument wird beschrieben, wie der DIA NAT Tracker und das Fallback auf Cisco IOS XE®-Routern mithilfe der Cisco Catalyst Manager-GUI konfiguriert und verifiziert werden.

## Voraussetzungen

### Anforderungen

Die Cisco SD-WAN NAT DIA-Richtlinie muss auf Geräten in Zweigstellen konfiguriert werden. Im Abschnitt [Zugehörige Informationen](#) finden Sie Anweisungen zur Implementierung von Direct Internet Access (DIA) für SD-WAN.

### Verwendete Komponenten

Dieses Dokument basiert auf den folgenden Software- und Hardwareversionen:

- Cisco Catalyst SD-WAN Manager Version 20.14.1

- Cisco Catalyst SD-WAN-Controller Version 20.14.1
- Cisco Edge Router Version 17.14.01a

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.

## Einschränkungen für NAT DIA Tracker

### Einschränkungen für Cisco IOS XE Catalyst SD-WAN Version 17.10.1a und frühere Versionen

- In Cisco IOS XE Version 17.6.x und früheren Versionen wird der NAT DIA Tracker nicht auf Dialer-Schnittstellen unterstützt. Ab Cisco IOS XE Catalyst SD-WAN Version 17.7.1a unterstützen Subschnittstellen und Dialer-Schnittstellen einen oder zwei Endpunkt-Tracker.
- DNS-URL-Endpunkte werden auf Cisco IOS XE Catalyst SD-WAN-Geräten nicht unterstützt.
- Sie können nur einen Tracker oder eine Tracker-Gruppe auf eine Schnittstelle anwenden.
- Die NAT-Fallback-Funktion wird nur von Cisco IOS XE Catalyst SD-WAN Version 17.3.2 unterstützt.
- Die IP-Adresse des Tunnels mit der Adresse 169.254.x.x wird für die Nachverfolgung des zScaler-Endpunkts in manuellen Tunneln nicht unterstützt.
- Sie müssen mindestens zwei einzelne Endpunkt-Tracker konfigurieren, um eine Tracker-Gruppe zu konfigurieren.
- Eine Tracker-Gruppe kann nur maximal zwei einzelne Endpoint-Tracker umfassen.
- In Cisco IOS XE Version 17.10.1 und früheren Versionen können Sie IPv4 Tracker nicht auf einer IPv6-Schnittstelle konfigurieren oder umgekehrt. Der Tracker ist nicht aktiv.

### Einschränkungen für Cisco IOS XE Catalyst SD-WAN Version 17.11.1a

- Der API-URL-Endpunkt wird nur für den IPv6-DIA-Tracker und nicht für den IPv4-DIA-Tracker unterstützt.
- IPv4- und IPv6-Tracker können nicht in derselben Tracker-Gruppe verwendet werden.
- Sie müssen den Befehl `allow service all` unter der TLOC-Tunnelschnittstelle konfigurieren, damit IPv6-Tracker mit einer TLOC-Tunnelschnittstelle arbeiten können.
- Mehrere NAT66-DIA-Schnittstellen werden nicht unterstützt.
- NAT-Fallback auf zentralisierte Datenrichtlinien wird nicht unterstützt.

### Einschränkungen für Cisco IOS XE Catalyst SD-WAN Version 17.13.1a

- Endpunkt-DNS-Elemente werden in einer Tracker-Gruppe nicht unterstützt.

---

Hinweis: Stellen Sie sicher, dass Sie eine Endpunkt-IP-Adresse verwenden, die auf HTTP/HTTPS-Anfragen antwortet. So kann beispielsweise der Google DNS-Server 8.8.8.8 nicht als IP-Adresse für Endgeräte verwendet werden.

---

## Unterstützte Schnittstellen für NAT DIA Tracker

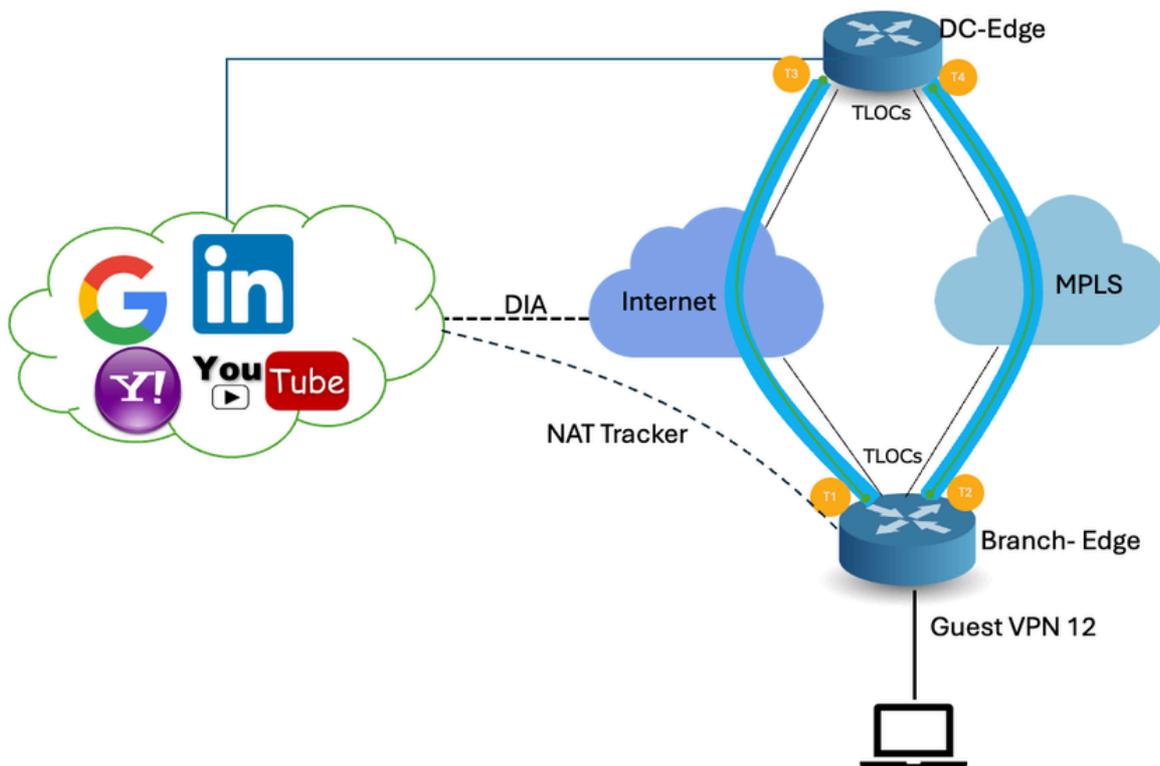
Sie können den NAT DIA Tracker für die folgenden Schnittstellen konfigurieren:

- Mobilfunkschnittstellen
- Ethernet-Schnittstellen
- Ethernet-Schnittstellen (PPPoE)
- Subschnittstellen
- DSL Dialer Interfaces (PPPoE und PPPoA)

Hinweis: Der IPv6 NAT DIA-Tracker wird nur auf physischen und Subschnittstellen von Ethernet-Schnittstellen unterstützt.

## Konfigurieren

### Netzwerkdiagramm



### Konfigurationen

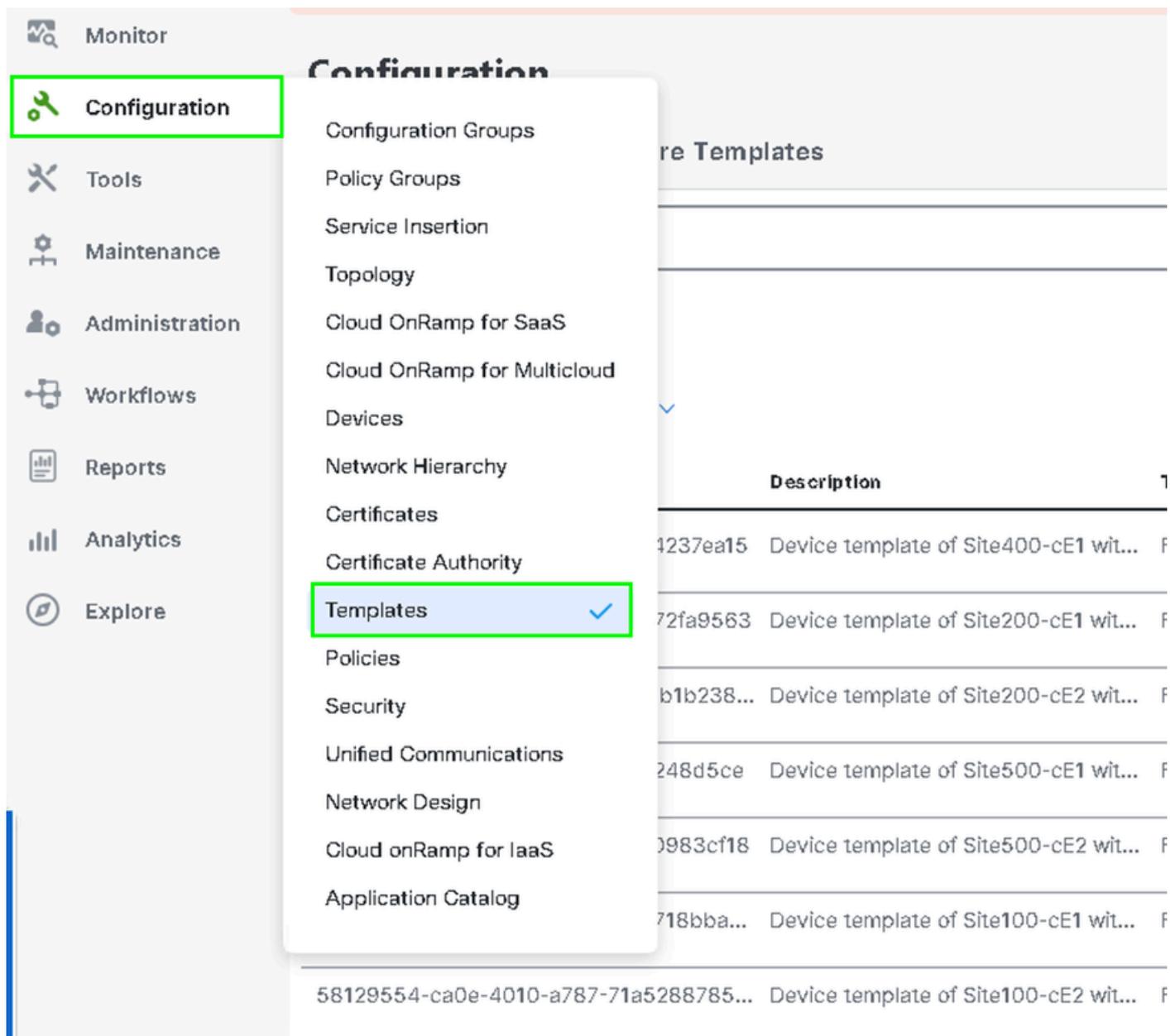
Der DIA-Tracker hilft festzustellen, ob das Internet oder ein externes Netzwerk nicht mehr verfügbar ist. Die NAT DIA Tracking-Funktion ist nützlich, wenn NAT auf einer Transportschnittstelle in VPN 0 aktiviert ist, damit der Datenverkehr vom Router direkt in das Internet übertragen werden kann.

Wenn das Internet oder ein externes Netzwerk nicht mehr verfügbar ist, leitet der Router den

Datenverkehr auf Basis der NAT-Route im Service-VPN weiter. An das Internet weitergeleiteter Datenverkehr wird verworfen. Um zu verhindern, dass der Internetdatenverkehr verloren geht, konfigurieren Sie den DIA Tracker auf dem Edge-Router so, dass der Status der Transportschnittstelle nachverfolgt wird. Der Tracker überprüft in regelmäßigen Abständen die Schnittstelle, um den Status des Internets zu ermitteln und die Daten an die mit dem Tracker verknüpften Anschlusspunkte zurückzugeben.

## Schritt 1: NAT DIA Tracker konfigurieren

Navigieren Sie im Menü Cisco SD-WAN Manager zu Configuration > Templates (Konfiguration > Vorlagen).



The screenshot shows the Cisco SD-WAN Manager interface. On the left, there is a navigation menu with the following items: Monitor, Configuration (highlighted with a green box), Tools, Maintenance, Administration, Workflows, Reports, Analytics, and Explore. A dropdown menu is open from the Configuration item, listing various configuration options: Configuration Groups, Policy Groups, Service Insertion, Topology, Cloud OnRamp for SaaS, Cloud OnRamp for Multicloud, Devices, Network Hierarchy, Certificates, Certificate Authority, Templates (highlighted with a green box and a blue checkmark), Policies, Security, Unified Communications, Network Design, Cloud onRamp for IaaS, and Application Catalog. In the background, a table titled 'Device Templates' is visible, showing a list of templates with columns for ID, Description, and Status.

ID	Description	Status
4237ea15	Device template of Site400-cE1 wit...	F
72fa9563	Device template of Site200-cE1 wit...	F
b1b238...	Device template of Site200-cE2 wit...	F
248d5ce	Device template of Site500-cE1 wit...	F
0983cf18	Device template of Site500-cE2 wit...	F
718bba...	Device template of Site100-cE1 wit...	F
58129554-ca0e-4010-a787-71a5288785...	Device template of Site100-cE2 wit...	F

Klicken Sie auf Funktionsvorlagen. Suchen Sie in der Suchleiste nach der Funktionsvorlage Cisco System, klicken Sie auf die drei Punkte (...) und dann auf Bearbeiten, um die Änderungen

vorzunehmen.

**Configuration**

Device Templates **Feature Templates**

Q 400 x system x Search

Add Template

Template Type Non-Default

Total Rows: 3 of 125

Name	Description	Type	Device Model	Device Templates	Devices Attached	Updated By	Last Updated
ntp_system_21*10*2021_19*3...	Test Drive Template: System ...	Cisco NTP	CSR1000v	8	8	admin	04 Apr 2024 7:19:47 PM GM
system_Site400-cE1_400_28...	Test Drive Template: System ...	Cisco System	C8000v	1	1	admin	04 Apr 2024 4:21:19 PM GM
system_Site500-cE2_500_14e...	Test Drive Template: System ...	Cisco System	C8000v	1	1	admin	04 Apr 2024 4:27:53

- View
- Edit**
- Change Device Models
- Delete
- Copy

Klicken Sie im Beispiel mit den Systemfunktionen auf Tracker.

**Configuration**

Device Templates **Feature Templates**

Feature Template > Cisco System > system\_Site400-cE1\_400\_288e91b4-e59e-4af4-92f8-847b4237ea15\_04-04-2024\_16-21-17

Device Type C8000v

Template Name\* system\_Site400-cE1\_400\_288e91b4-e59e-4af4-

Description\* Test Drive Template: System feature of Site40C

Basic Configuration GPS **Tracker** Advanced

BASIC CONFIGURATION

Klicken Sie auf New Endpoint Tracker, um die Tracker-Parameter zu konfigurieren.

Tracker

TRACKERS TRACKER GROUPS

**New Endpoint Tracker**

Optional	Name	Threshold	Interval	Multiplier	Tracker Type
No data available					

Geben Sie die Tracker-Parameter ein, und klicken Sie auf Hinzufügen.

Name: Name des Trackers. Der Name kann bis zu 128 alphanumerische Zeichen enthalten. Sie können bis zu acht Tracker konfigurieren.

Grenzwert: Dauer, die gewartet wird, bis der Prüfpunkt eine Antwort zurückgibt, bevor erklärt wird, dass die Transportschnittstelle ausgefallen ist. Bereich: 100 bis 1000 Millisekunden. Standard: 300 Millisekunden.

Intervall (Intervall): Häufigkeit, mit der ein Prüfpunkt gesendet wird, um den Status der Transportschnittstelle zu bestimmen. Bereich: 20 bis 600 Sekunden. Standard: 60 Sekunden (1 Minute).

Multipliiert (Multiplikator): Anzahl der Male, die eine Anfrage erneut gesendet werden kann, bevor erklärt wird, dass die Transportschnittstelle ausgefallen ist. Bereich: 1 bis 10. Standard: 3.

Tracker-Typ: Wählen Sie Interface (Schnittstelle) aus, um den DIA-Tracker zu konfigurieren.

Endpunkttyp: Sie können eine IP-Adresse, einen DNS-Namen oder eine URL auswählen.

Endpunkt-DNS-Name: DNS-Name des Endpunkts. Dies ist das Ziel im Internet, an das der Router Tests sendet, um den Status der Transportschnittstelle zu bestimmen.

Klicken Sie auf das Dropdown-Menü, und wählen Sie Global aus, um einen beliebigen Standardwert zu ändern.

The screenshot shows a configuration window titled 'Tracker' with a dropdown menu. Below the title, there are two tabs: 'TRACKERS' and 'TRACKER GROUPS'. A 'New Endpoint Tracker' button is visible. The form contains several fields:

- Name:** A text input field containing 'tracker1'.
- Threshold:** A numeric input field containing '300'.
- Interval:** A dropdown menu with 'Global' selected.
- Multiplier:** A dropdown menu with 'Default' selected.
- Tracker Type:** A dropdown menu with 'interface' selected.
- Endpoint Type:** Radio buttons for 'IP Address', 'DNS Name' (selected), and 'URL'.
- Endpoint DNS Name:** A text input field containing 'www.cisco.com'.

At the bottom right, there are 'Cancel' and 'Add' buttons.

Klicken Sie auf Aktualisieren.

New Endpoint Tracker

Optional	Name	Threshold	Interval	Multiplier	Tracker Type	Action
<input type="checkbox"/>	<input type="text" value="tracker1"/>	<input type="text" value="100"/>	<input type="text" value="30"/>	<input type="text" value="3"/>	<input type="text" value="interface"/>	 

New Object Tracker

Mark as Optional Row

Tracker Type

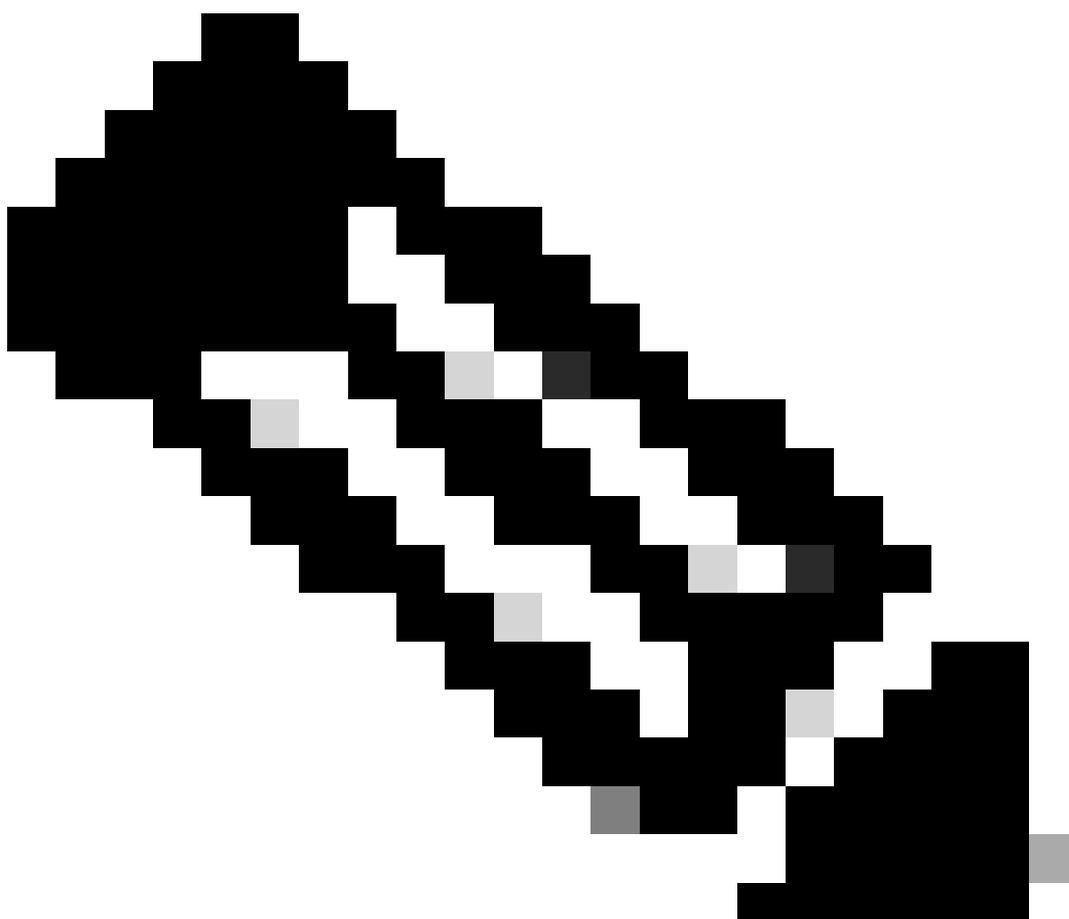
Interface  SIG  Route

Object ID

Interface

Cancel

Update



Hinweis: Stellen Sie sicher, dass Sie zwei einzelne Endpunkt-Tracker konfiguriert haben, bevor Sie eine Tracker-Gruppe konfigurieren.

Klicken Sie auf Next (Weiter).

Device Template | 288e91b4-e59e-4af4-92f8-847b4237ea15

Search

Total Rows: 1

S...	Chassis Number	System IP	Hostname	Prefix(0.0.0.0/0)	Address(192.168.1.1)	Interface Name(GigabitEthernet8)	IPv4 Address/ prefix-k
✓	C8K08B43DFE-2350-F2B2-E8E2-F80...		Site400-cE1	0.0.0.0/0		GigabitEthernet8	...

Next Cancel

Klicken Sie auf Geräte, und stellen Sie sicher, dass die Konfiguration korrekt ist. Klicken Sie auf Config Diff (Konfigurationsdiff) und auf Side by Side Diff (Nebeneinander). Klicken Sie auf Geräte konfigurieren.

Device Template | 288e91b4-e59e-4af4-9... | Total 1

Device list (Total: 1 devices)

Filter/Search

C8K-08B43DFE-2350-F2B2-E8E2-F8CF3EDD8887  
Site400-cE1|11.40.1  
Configure Devi...

Config Preview | **Config Diff**

```
system
ztp-status in-progress
device-model vedge-C8000V
gps-location latitude 19.04674
gps-location longitude 72.85223
system-ip
overlay-id 1
site-id 400
no transport-gateway enable
port-offset 0
control-session-pps 300
admin-tech-on-failure
sp-organization-name Viptela-POC-Tool
organization-name Viptela-POC-Tool
```

333	no crypto ikev2 diagnose error	333	endpoint-tracker tracker1
334	no crypto isakmp diagnose error	334	tracker-type interface
335	no network-clock revertive	335	endpoint-dns-name www.cisco.com
336	snmp-server ifindex persist	336	threshold 100
337	fhrp version vrrp v2	337	interval 30
338	line con 0	338	!
339	speed 115200	339	no crypto ikev2 diagnose error
340	stopbits 1	340	no crypto isakmp diagnose error
341	!	341	no network-clock revertive
342	line vty 0 4	342	snmp-server ifindex persist
343	transport input ssh	343	fhrp version vrrp v2
344	!	344	line con 0
345	line vty 5 80	345	speed 115200
		346	stopbits 1
		347	!
		348	line vty 0 4
		349	transport input ssh
		350	!
		351	line vty 5 80

Back Configure Devices Cancel

vManage hat die Gerätevorlage erfolgreich mit der Tracker-Konfiguration konfiguriert.

Push Feature Template Configuration | ● Validation success

Total Task: 1 | Success : 1

Device Group (1)

Q Search Table

Status	Message	Chassis Number
● Success	Template successfully attac...	

### View Logs

Host: Site400-cE1( )

Site ID: 400

Device C8000v

Model:

[29-Jul-2024 7:50:20 PDT] Configuring device with feature template:

[29-Jul-2024 7:50:21 PDT] Checking and creating device in Manager

[29-Jul-2024 7:50:22 PDT] Generating configuration from template

[29-Jul-2024 7:50:29 PDT] Device is online

[29-Jul-2024 7:50:29 PDT] Updating device configuration in Manager

[29-Jul-2024 7:50:29 PDT] Sending configuration to device

[29-Jul-2024 7:50:36 PDT] Successfully notified device to pull configuration

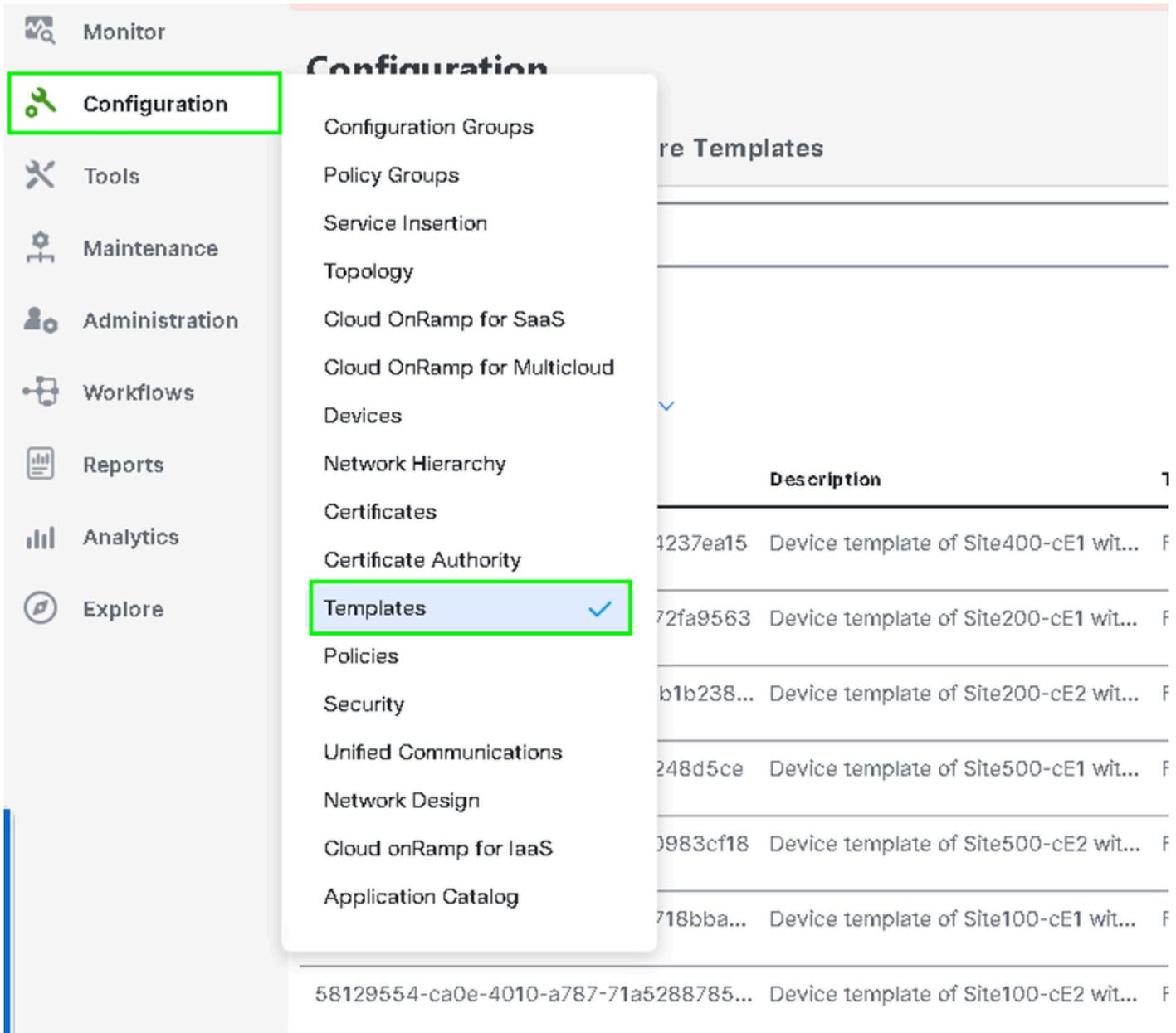
[29-Jul-2024 7:50:36 PDT] Device has pulled the configuration

[29-Jul-2024 7:50:39 PDT] Device: Config applied successfully

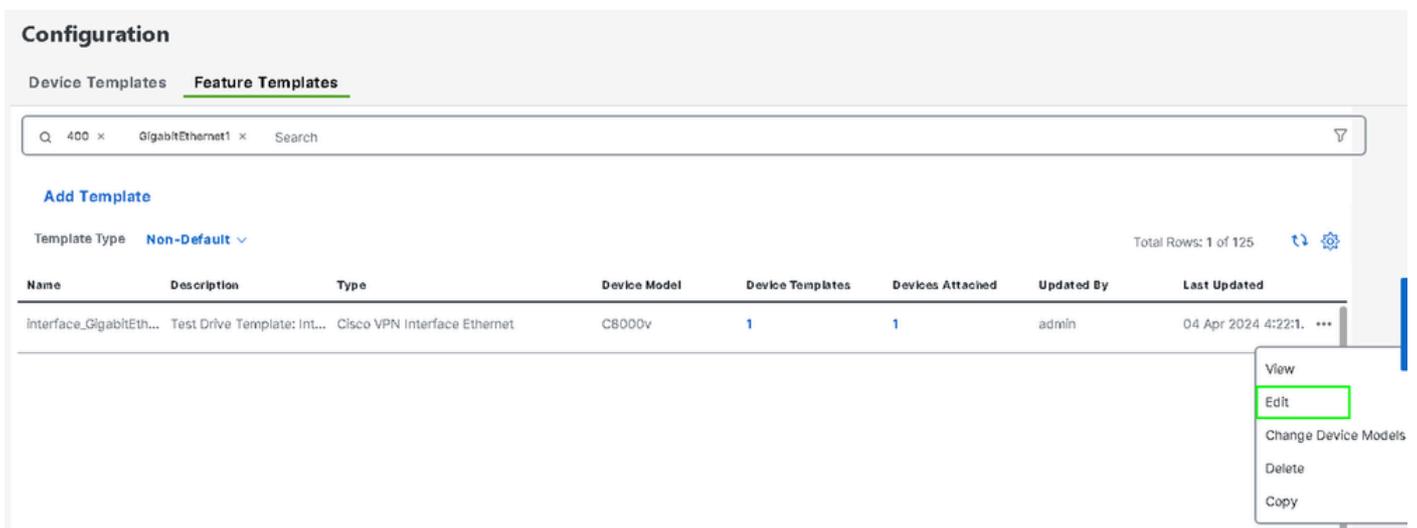
[29-Jul-2024 7:50:39 PDT] Template successfully attached to device

## Schritt 2: Anbinden des Trackers an die Transportschnittstelle

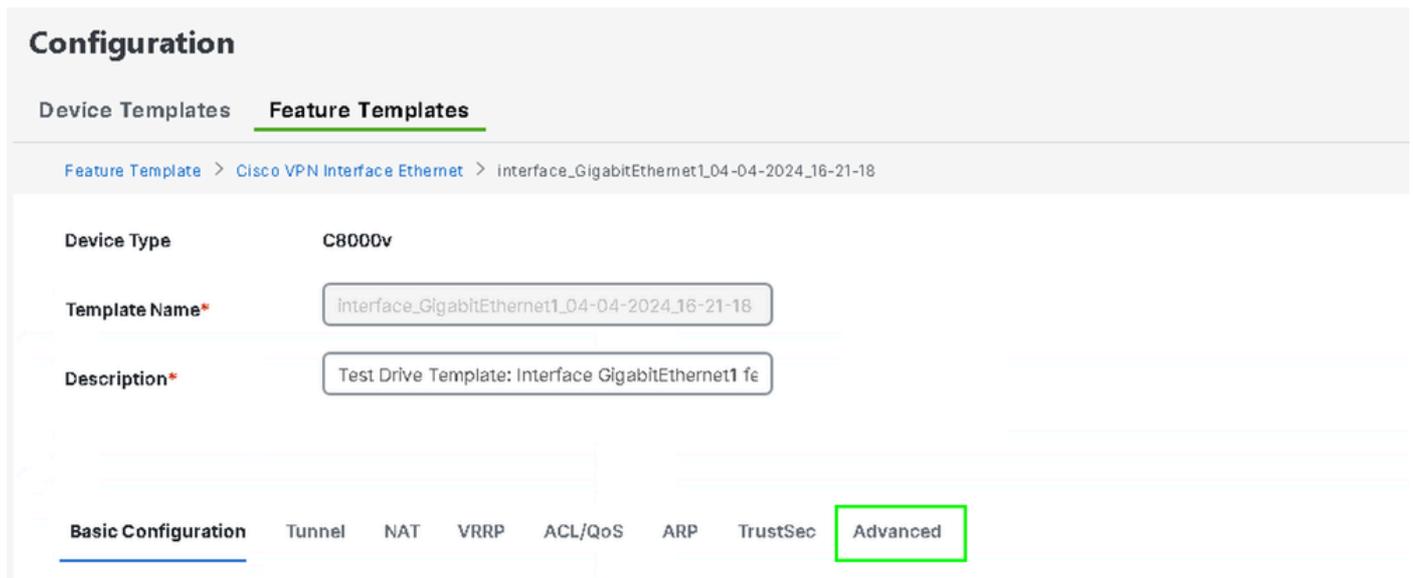
Navigieren Sie im Menü Cisco SD-WAN Manager zu Configuration > Templates (Konfiguration > Vorlagen).



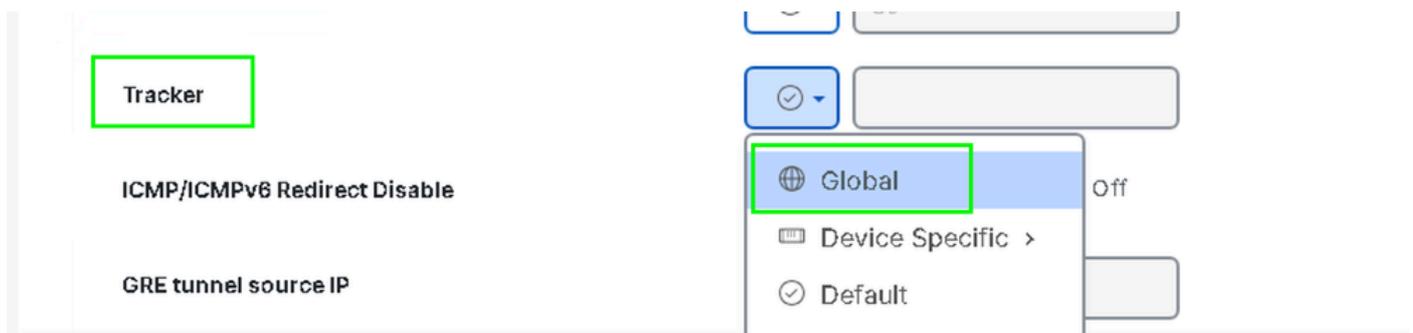
Suchen Sie in der Suchleiste nach der Funktionsvorlage NAT Transport Interface, klicken Sie auf die drei Punkte (...), und klicken Sie zum Ändern auf Edit.



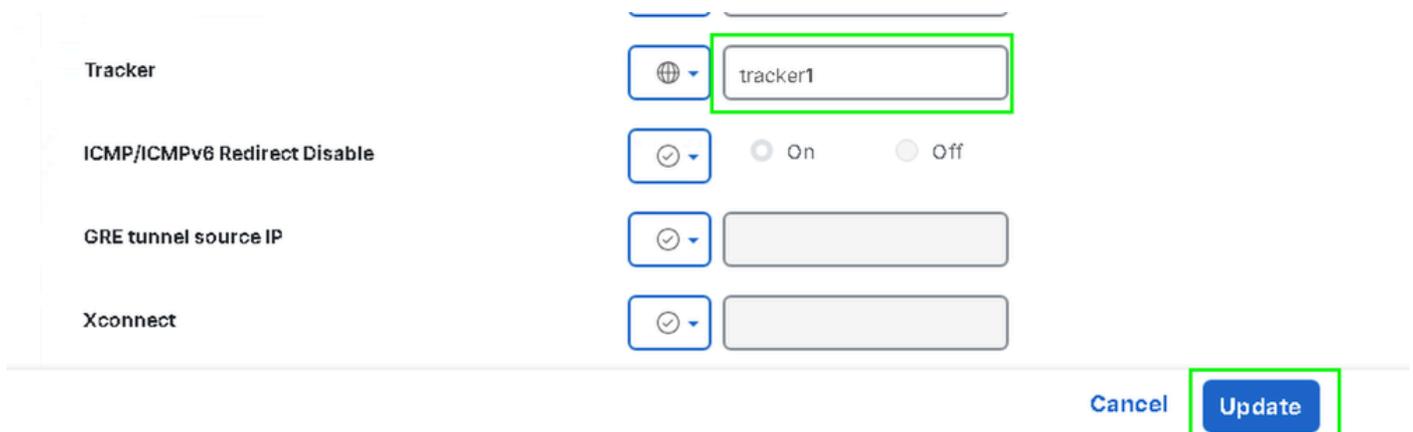
Klicken Sie auf die Registerkarte Advanced (Erweitert).



Um den Tracker-Namen zum Tracker hinzuzufügen, wählen Sie Global aus dem Dropdown-Menü aus.



Geben Sie den Tracker-Namen ein, den Sie in der Systemvorlage erstellt haben, und klicken Sie auf Aktualisieren.



Klicken Sie auf Next (Weiter).

Device Template | 288e91b4-e59e-4af4-92f8-847b4237ea15

Q Search

Total Rows: 1

S...	Chassis Number	System IP	Hostname	Prefix(0.0.0.0/0)	Address(192.168.1.1)	Interface Name(GigabitEthernet8)	IPv4 Address/ prefix-k
✓	C8K-08B43DFE-2350-F2B2-E8E2-F80...		Site400-cE1	0.0.0.0/0		GigabitEthernet8	...

Next Cancel

Klicken Sie auf Geräte, und stellen Sie sicher, dass die Konfiguration korrekt ist. Klicken Sie auf Config Diff (Konfigurationsdiff) und auf Side by Side Diff (Nebeneinander). Klicken Sie auf Geräte konfigurieren.

Device Template | 288e91b4-e59e-4af4-9... | Total 1

Device list (Total: 1 devices)

Filter/Search

C8K-08B43DFE-2350-F2B2-E8E2-F80F3EDDB887  
Site400-cE1|1.1.40.1

Configure Devi...

Config Preview | **Config Diff**

```

system
ztp-status          in-progress
device-model        vedge-C8000V
gps-location latitude 19.04674
gps-location longitude 72.85223
system-ip
overlay-id          1
site-id             400
no transport-gateway enable
port-offset         0
control-session-pps 300
admin-tech-on-failure
sp-organization-name Viptela-POC-Tool
organization-name   Viptela-POC-Tool
port-hop
track-transport
track-default-gateway
console-baud-rate   115200
no on-demand enable
on-demand idle-timeout 10
  
```

interface GigabitEthernet1	212	interface GigabitEthernet1
no shutdown	213	no shutdown
arp timeout 1200	214	arp timeout 1200
ip address 10.2.7.2 255.255.255.0	215	ip address 10.2.7.2 255.255.255.0
no ip redirects	216	no ip redirects
ip mtu 1500	217	ip mtu 1500
ip nat outside	218	ip nat outside
load-interval 30	219	load-interval 30
mtu 1500	220	mtu 1500
	221	endpoint-tracker tracker1
negotiation auto	222	negotiation auto
exit	223	exit
interface GigabitEthernet2	224	interface GigabitEthernet2
no shutdown	225	no shutdown
arp timeout 1200	226	arp timeout 1200

Back
Configure Devices
Cancel

vManage hat die Gerätevorlage erfolgreich konfiguriert.

Push Feature Template Configuration | ● Validation success

Total Task: 1 | Success: 1

Device Group (1)

Q Search Table

Status	Message	Chassis Number
● Success	Template successfully attac...	

### View Logs

Host: Site400-cE1( )

Site ID: 400

Device: C8000v

Model:

[29-Jul-2024 8:02:13 PDT] Configuring device with feature template:

[29-Jul-2024 8:02:13 PDT] Checking and creating device in Manager

[29-Jul-2024 8:02:14 PDT] Generating configuration from template

[29-Jul-2024 8:02:20 PDT] Device is online

[29-Jul-2024 8:02:20 PDT] Updating device configuration in Manager

[29-Jul-2024 8:02:21 PDT] Sending configuration to device

[29-Jul-2024 8:02:26 PDT] Successfully notified device to pull configuration

[29-Jul-2024 8:02:26 PDT] Device has pulled the configuration

[29-Jul-2024 8:02:29 PDT] Device: Config applied successfully

[29-Jul-2024 8:02:29 PDT] Template successfully attached to device

### Schritt 3: NAT-Fallback für vorhandene DIA-Richtlinie aktivieren

Cisco IOS XE Catalyst SD-WAN-Geräte unterstützen die NAT-Fallback-Funktion für Direct Internet Access (DIA). Die NAT-Fallback-Funktion ermöglicht es dem Datenverkehr, einen alternativen Pfad zu verwenden, wenn der primäre NAT-Pfad ausfällt. Dadurch wird eine kontinuierliche Anbindung auch bei Problemen mit der primären NAT-Konfiguration gewährleistet.

So aktivieren Sie NAT-Fallback mit Cisco SD-WAN Manager:

Navigieren Sie im Menü Cisco SD-WAN Manager zu Konfiguration > Richtlinie.



Monitor



Configuration



Tools



Maintenance



Administration



Workflows



Reports



Analytics



Explore

Configuration Groups

Policy Groups

Service Insertion

Topology

Cloud OnRamp for SaaS

Cloud OnRamp for Multicloud

Devices

Network Hierarchy

Certificates

Certificate Authority

Templates

Policies ✓

Security

Unified Communications

Network Design

Cloud onRamp for IaaS

Application Catalog

VIP10\_DC\_Preference

VIP16\_QoS\_Classify\_SIP

```

interface GigabitEthernet1
ip address 10.2.7.2 255.255.255.0
no ip redirects
ip nat outside
load-interval 30
negotiation auto

endpoint-tracker tracker1

arp timeout 1200
end

```

```

Site400-cE1#show sdwan running-config | sec endpoint
endpoint-tracker tracker1
tracker-type interface
endpoint-dns-name www.cisco.com
threshold 100
interval 30

```

Die Ausgabe zeigt, wie der Tracker-Status mithilfe der Befehle show endpoint-tracker und show endpoint-tracker GigabitEthernet1 überprüft wird.

```

Site400-cE1#show endpoint-tracker
Interface      Record Name  Status  Address Family  RTT in msec  Probe ID  Next Hop
GigabitEthernet1  tracker1    Up      IPv4             8             6         10.2.7.1

Site400-cE1#show endpoint-tracker interface GigabitEthernet1
Interface      Record Name  Status  Address Family  RTT in msec  Probe ID  Next Hop
GigabitEthernet1  tracker1    Up      IPv4             8             6         10.2.7.1

```

Die Ausgabe zeigt zeitgeberbezogene Informationen über den Tracker an, um bei der Fehlerbehebung von Problemen im Zusammenhang mit dem Tracker zu helfen, sofern vorhanden:

```

Site400-cE1#show endpoint-tracker records
Record Name  Endpoint      EndPoint Type  Threshold(ms)  Multiplier  Interval(s)  Tracker-Type
tracker1     www.cisco.com  DNS_NAME      100             3           30           interface

```

Die Ausgabe von show ip sla summarycommand.

```

Site400-cE1#show ip sla summary
IPSLAs Latest Operation Summary
Codes: * active, ^ inactive, ~ pending

```

All Stats are in milliseconds. Stats with u are in microseconds

ID	Type	Destination	Stats	Return Code	Last Run
*5	dns	8.8.8.8	RTT=16	OK	16 seconds ago
*6	http	x.x.x.x	RTT=15	OK	3 seconds ago

Überprüfen Sie die Fallback-Konfiguration, die auf das Gerät angewendet wurde, mithilfe des Befehls `show sdwan policy from-vsmart`.

<#root>

```
Site400-cE1#show sdwan policy from-vsmart
from-vsmart data-policy _VPN12_VPN12_DIA
direction from-service
vpn-list VPN12
sequence 1
match
source-data-prefix-list Site400_AllVPN_Prefixes
action accept
nat use-vpn 0

nat fallback

no nat bypass
default-action drop
```

## Tracker zur Fehlerbehebung

Aktivieren Sie diese Debugging-Funktionen auf dem Edge-Gerät, um zu überprüfen, wie der Router Tests sendet, um den Status der Transportschnittstelle zu bestimmen.

- Um zu überwachen, wie der Router Tests sendet und den Status der Transportschnittstellen feststellt, verwenden Sie den Befehl `sdwan tracker` der Debug-Plattform, der bis zur Version 17.12.x unterstützt wird.
- Aktivieren Sie ab 17.13.x diese Debugging-Optionen, um die Prüfprotokolle zu überwachen.
  - `set platform software trace ios R0 sdwanrp-tracker debuggen`
  - `set platform software trace ios R0 sdwanrp-cfg debug`
- Um die Protokolle zu überprüfen, die sich auf Fehler und Ablaufverfolgung bei IP SLA-Vorgängen beziehen, aktivieren Sie diese Debugging-Optionen. Diese Protokolle zeigen an, ob IP SLA-Vorgänge fehlschlagen.
  - `debug ip sla trace`
  - `debug ip sla error`

Führen Sie die folgenden Befehle aus, um die Debug-Protokolle zu überprüfen:

- `show logging profile sdwan intern`

- sdwan internes Überwachungsprotokollierungsprofil

Site400-cE1#show logging profile sdwan internal

Logging display requested on 2024/08/13 08:10:45 (PDT) for Hostname: [Site400-cE1], Model: [C8000V], Ve

Displaying logs from the last 0 days, 0 hours, 10 minutes, 0 seconds

executing cmd on chassis local ...

Unified Decoder Library Init .. DONE

Found 1 UTF Streams

```
2024/08/13 08:02:28.408998337 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:10 s
2024/08/13 08:02:28.409061529 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:10 S
2024/08/13 08:02:28.409086404 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE: Sla sync
2024/08/13 08:02:28.409160541 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE: Sla sync
2024/08/13 08:02:28.409182208 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 St
2024/08/13 08:02:28.409197024 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 Qu
2024/08/13 08:02:28.409215496 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 DN
2024/08/13 08:02:28.409242243 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 So
2024/08/13 08:02:28.409274690 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 So
2024/08/13 08:02:28.409298157 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 So
2024/08/13 08:02:28.409377223 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 Ne
2024/08/13 08:02:28.409391034 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 Re
2024/08/13 08:02:28.409434969 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 ac
2024/08/13 08:02:28.409525831 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 Pr
2024/08/13 08:02:28.426966448 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 Qu
2024/08/13 08:02:28.427004143 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 Re
2024/08/13 08:02:28.427029754 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 RT
2024/08/13 08:02:28.427161550 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:10 S
2024/08/13 08:02:28.427177727 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:10 S
2024/08/13 08:02:28.427188035 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:10 S
2024/08/13 08:02:28.427199147 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:10 S
2024/08/13 08:02:28.427208941 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 IP
2024/08/13 08:02:28.427219960 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common St
2024/08/13 08:02:28.427238042 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common St
2024/08/13 08:02:28.427301952 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common St
2024/08/13 08:02:28.427316275 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common St
2024/08/13 08:02:28.427326235 {iosrp_R0-0}{255}: [sdwanrp-tracker] [17432]: (debug): Received IPSLA sta
2024/08/13 08:02:28.427328425 {iosrp_R0-0}{255}: [sdwanrp-tracker] [17432]: (debug): DNS status callbac
2024/08/13 08:02:28.427341452 {iosrp_R0-0}{255}: [sdwanrp-tracker] [17432]: (debug): DNS query valid TR
2024/08/13 08:02:28.427343152 {iosrp_R0-0}{255}: [sdwanrp-tracker] [17432]: (debug): DNS resolved addre
2024/08/13 08:02:28.427344332 {iosrp_R0-0}{255}: [sdwanrp-tracker] [17432]: (debug): DNS probe handler
2024/08/13 08:02:28.427349194 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:10 S
2024/08/13 08:02:28.427359268 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common St
2024/08/13 08:02:28.427370416 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common St
2024/08/13 08:02:28.427555382 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common St
2024/08/13 08:02:28.427565670 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:10 S
2024/08/13 08:02:28.427577691 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common St
2024/08/13 08:02:28.427588947 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common St
2024/08/13 08:02:28.427600567 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common St
2024/08/13 08:02:28.427611465 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common St
2024/08/13 08:02:28.427620724 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:10 S
2024/08/13 08:02:28.427645035 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:10 S
2024/08/13 08:02:55.599896668 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:3 sI
2024/08/13 08:02:55.599966240 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:3 St
2024/08/13 08:02:55.599981173 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 Sta
2024/08/13 08:02:55.600045761 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 Nex
2024/08/13 08:02:55.600111585 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 DNS
2024/08/13 08:02:55.600330868 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 sla
2024/08/13 08:02:55.610693565 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 Soc
2024/08/13 08:02:55.610717011 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 Wai
```

```
2024/08/13 08:02:55.610777327 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 Sen
2024/08/13 08:02:55.610788233 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 Wai
2024/08/13 08:02:55.618534651 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 Soc
2024/08/13 08:02:55.618685838 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 HTT
2024/08/13 08:02:55.618697389 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:3 Sc
2024/08/13 08:02:55.618706090 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:3 Sc
2024/08/13 08:02:55.618714316 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:3 Sc
2024/08/13 08:02:55.618723915 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:3 Sc
2024/08/13 08:02:55.618732815 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 IPS
2024/08/13 08:02:55.618821650 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common St
2024/08/13 08:02:55.618833396 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common St
2024/08/13 08:02:55.618857012 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common St
```

## Zugehörige Informationen

[Implementierung von Direct Internet Access \(DIA\) für SD-WAN](#)

[Cisco Catalyst SD-WAN NAT - Konfigurationsleitfaden](#)

[NAT-Fallback auf Cisco IOS XE Catalyst SD-WAN-Geräten](#)

[Technischer Support und Dokumentation für Cisco Systeme](#)

## 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.