配置并检验DIA NAT跟踪器和回退

目录

简介

先决条件

- 要求
- 使用的组件
- NAT DIA跟踪器的限制
  - Cisco IOS XE Catalyst SD-WAN版本17.10.1a及更早版本的限制
  - Cisco IOS XE Catalyst SD-WAN版本17.11.1a的限制
  - Cisco IOS XE Catalyst SD-WAN版本17.13.1a的限制
- NAT DIA跟踪器支持的接口

配置

- 网络图
- 配置
- 步骤1.配置NAT DIA跟踪器
- 步骤2.将跟踪器绑定到传输接口
- 步骤3.在现有DIA策略上启用NAT回退

验证

故障排除跟踪器

相关信息

简介

本文档介绍如何使用Cisco Catalyst Manager GUI在CIsco IOS® XE路由器上配置和验证DIA NAT Tracker和Fallback。

先决条件

要求

必须在分支机构设备上配置思科SD-WAN NAT DIA策略。请查看相关信息部分，了解有关如何为SD-WAN实施直接互联网访问(DIA)的说明。

使用的组件

本文档基于以下软件和硬件版本：

- 思科Catalyst SD-WAN管理器20.14.1版
- 思科Catalyst SD-WAN控制器版本20.14.1
- 思科边缘路由器版本17.14.01a

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

NAT DIA跟踪器的限制

Cisco IOS XE Catalyst SD-WAN版本17.10.1a及更早版本的限制

- 在Cisco IOS XE版本17.6.x及更早版本中，拨号程序接口不支持NAT DIA跟踪器。在Cisco IOS XE Catalyst SD-WAN版本17.7.1a中，子接口和拨号器接口支持单终端和双终端跟踪器。
- Cisco IOS XE Catalyst SD-WAN设备不支持DNS URL终端。
- 只能将一个跟踪器或跟踪器组应用于接口。
- 仅Cisco IOS XE Catalyst SD-WAN版本17.3.2支持NAT回退功能。
- 不支持地址为169.254.x.x的隧道的IP地址在手动隧道上跟踪zScaler终端。
- 必须至少配置两个单个终端跟踪器才能配置跟踪器组。
- 跟踪器组最多只能包含两个单个终端跟踪器。
- 在Cisco IOS XE版本17.10.1和以前版本中，不能在IPv6接口上配置IPv4跟踪器，反之亦然。跟踪器不会处于活动状态。

Cisco IOS XE Catalyst SD-WAN版本17.11.1a的限制

- 仅IPv6 DIA跟踪器支持API URL终端，IPv4 DIA跟踪器不支持API URL终端。
- IPv4和IPv6跟踪器不能用于同一跟踪器组。
- 您必须在TLOC隧道接口下配置allow service all命令，IPv6跟踪器才能使用TLOC隧道接口。
- 不支持多个NAT66 DIA接口。

Cisco IOS XE Catalyst SD-WAN版本17.13.1a的限制

- 名称解析进程未绑定到ET接口。名称解析使用VPN 0路由表。它可以通过正确的路由退出任何活动接口。

NAT DIA跟踪器支持的接口

您可以为这些接口配置NAT DIA跟踪器：

- 蜂窝网接口

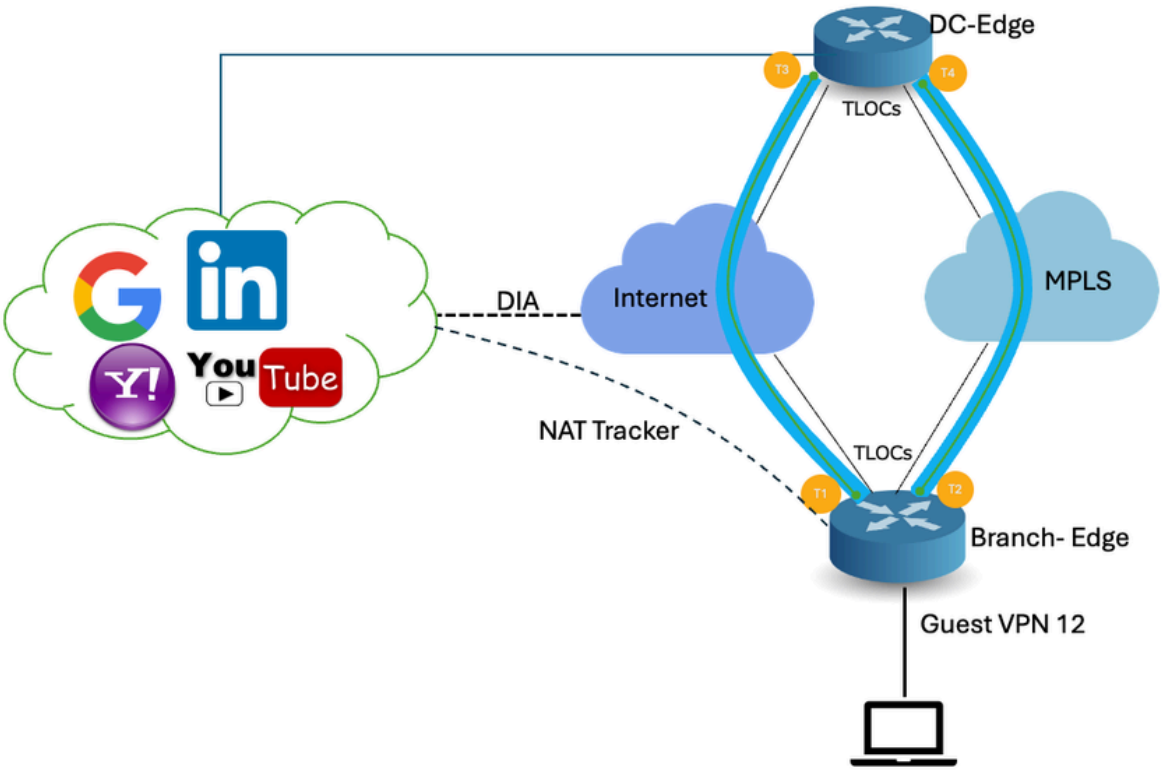
  注意：蜂窝接口不支持协商的IP地址。

- 以太网接口
- 以太网(PPPoE)接口
- 子接口
- DSL拨号器接口（PPPoE和PPPoA）

注意：IPv6 NAT DIA跟踪器仅在以太网接口的物理接口和子接口上受支持。

配置

网络图



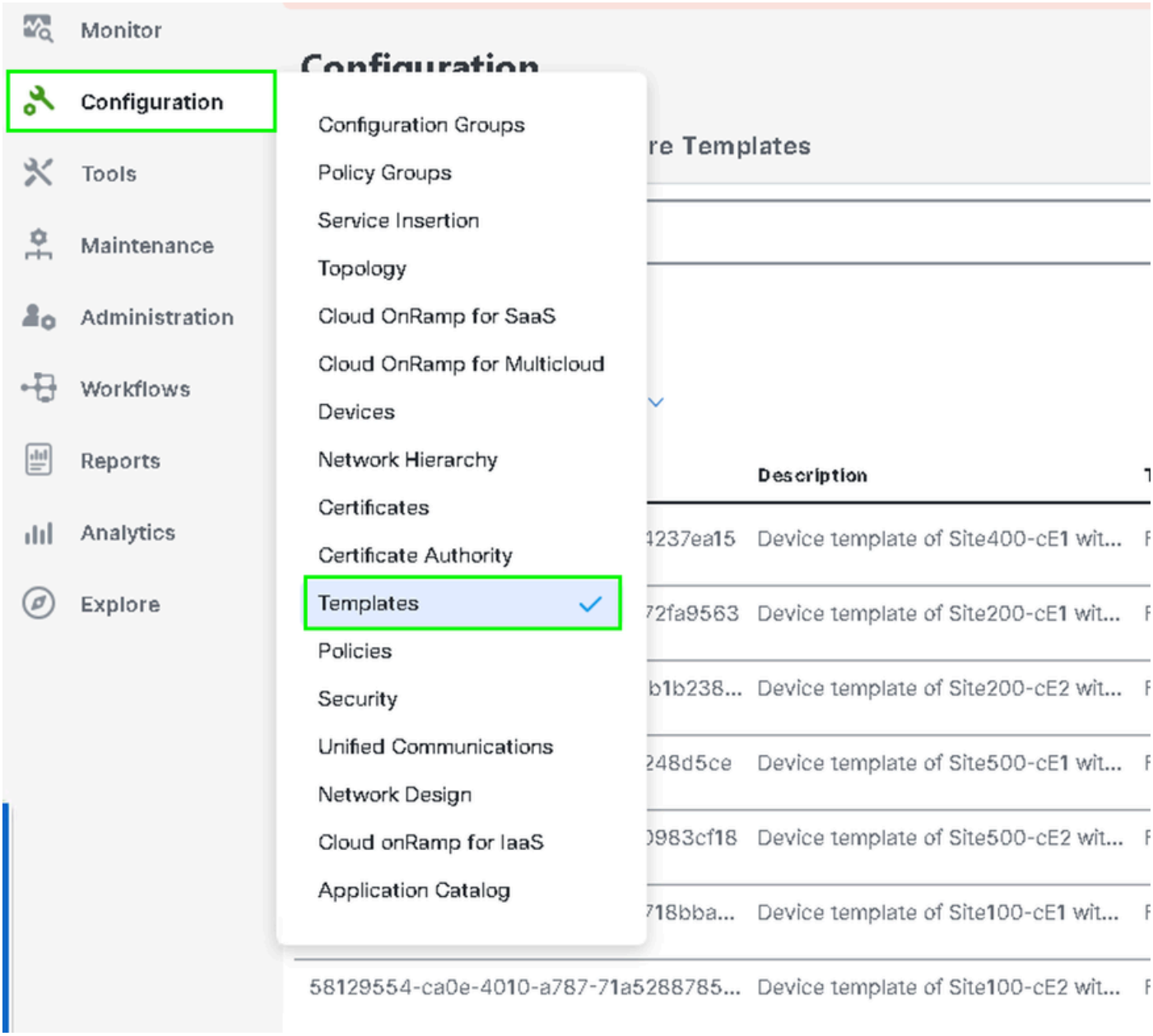
配置

DIA跟踪器有助于确定互联网或外部网络是否变得不可用。当VPN 0中的传输接口上启用NAT以允许来自路由器的数据流量直接退出到互联网时，NAT DIA跟踪功能非常有用。

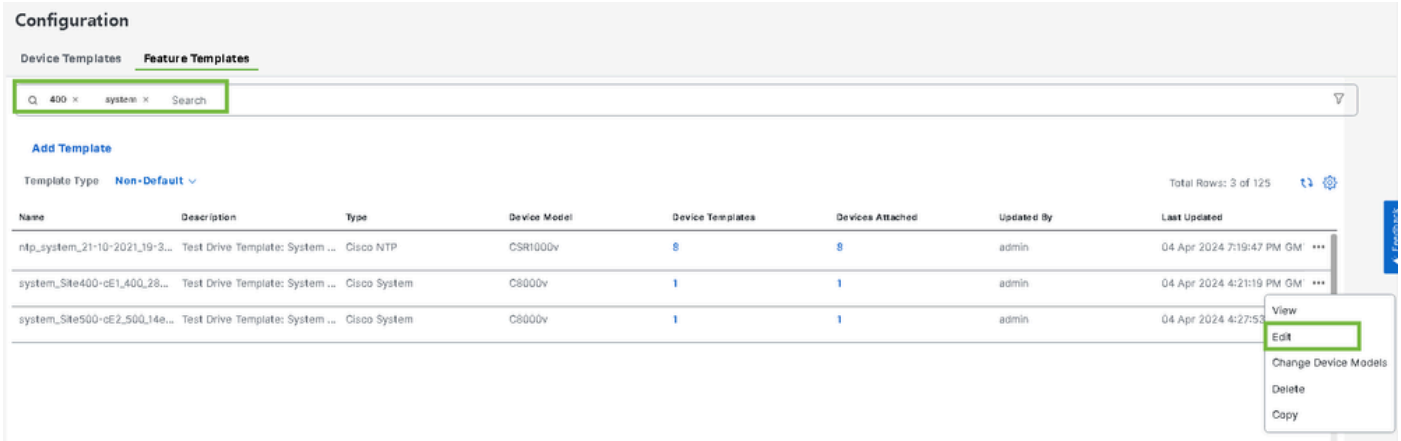
如果互联网或外部网络不可用，路由器会继续根据服务VPN中的NAT路由转发流量。转发到Internet的流量会被丢弃。为防止丢弃互联网绑定的流量，请在边缘路由器上配置DIA跟踪器以跟踪传输接口的状态。跟踪器会定期探测接口以确定互联网的状态，并将数据返回到与跟踪器关联的连接点。

步骤1.配置NAT DIA跟踪器

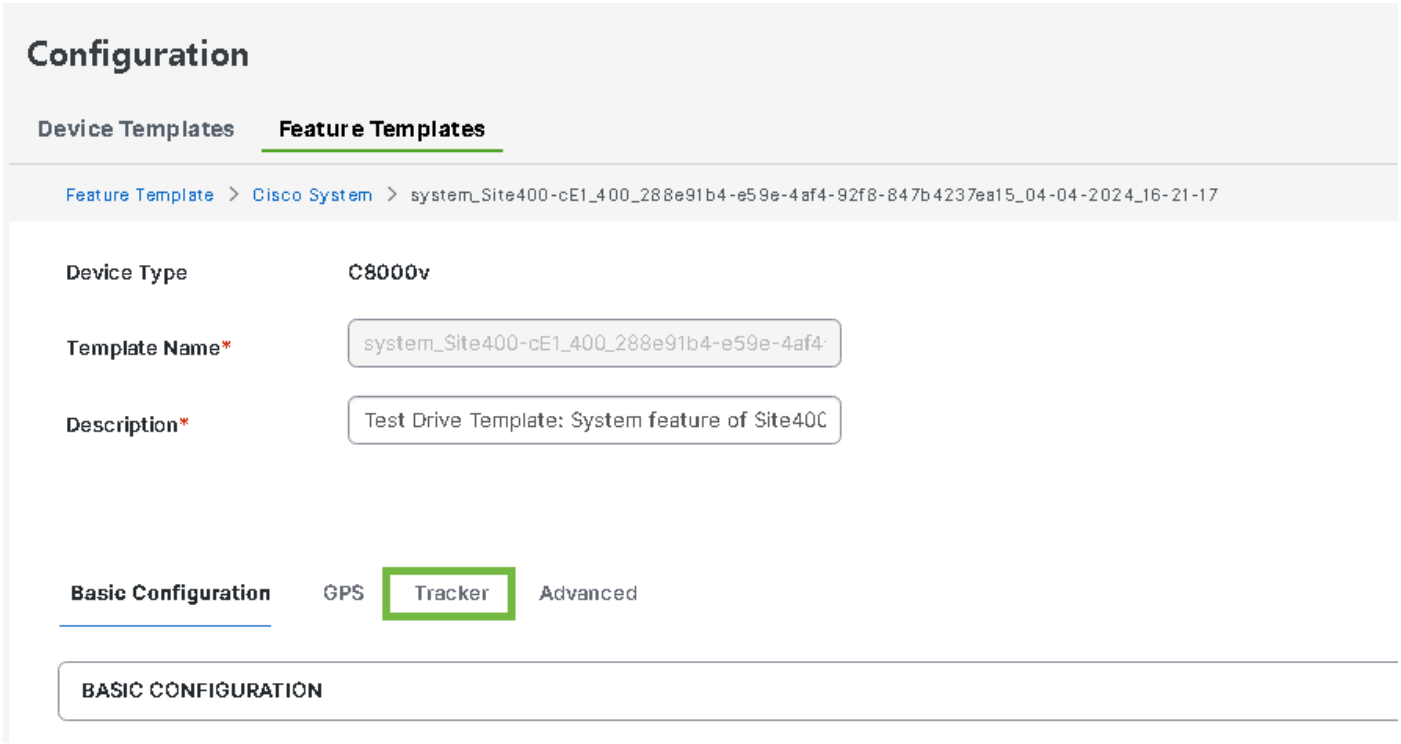
在Cisco SD-WAN Manager菜单中，导航至Configuration > Templates。



单击Feature Templates。在搜索栏中搜索Cisco System功能模板，单击三个点(...)，然后单击Edit进行修改。



在“系统”功能模板中，单击跟踪器。



单击New Endpoint Tracker配置跟踪器参数。



输入跟踪器参数，然后点击Add。

名称：跟踪器的名称。名称最多可包含128个字母数字字符。您最多可以配置八个跟踪器。

阈值:在声明传输接口关闭之前等待探测返回响应的持续时间。范围：100到1000毫秒。默认:300毫秒。

间隔:发送探测以确定传输接口状态的频率。范围：20到600秒。默认:60秒（1分钟）。

乘数：在声明传输接口关闭之前可以重新发送探测的次数。范围：1到10。默认值：3.

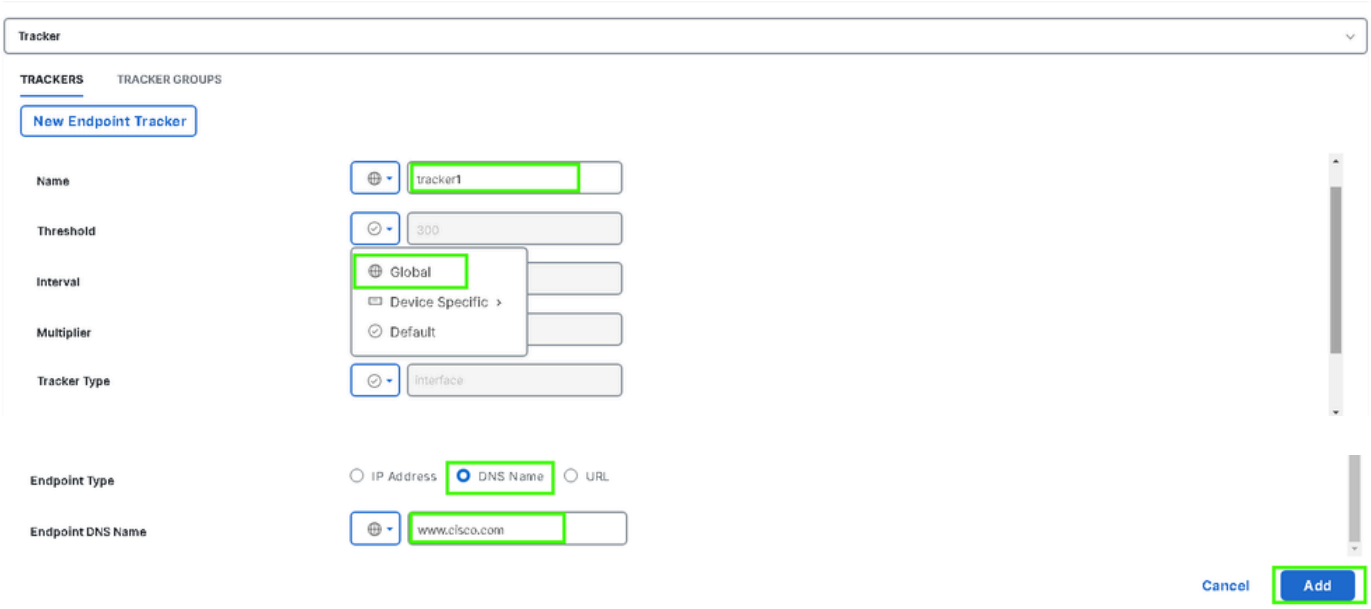
跟踪器类型：选择Interface以配置DIA跟踪器。

终端类型(End Point Type)：您可以选择IP地址、DNS名称或URL。

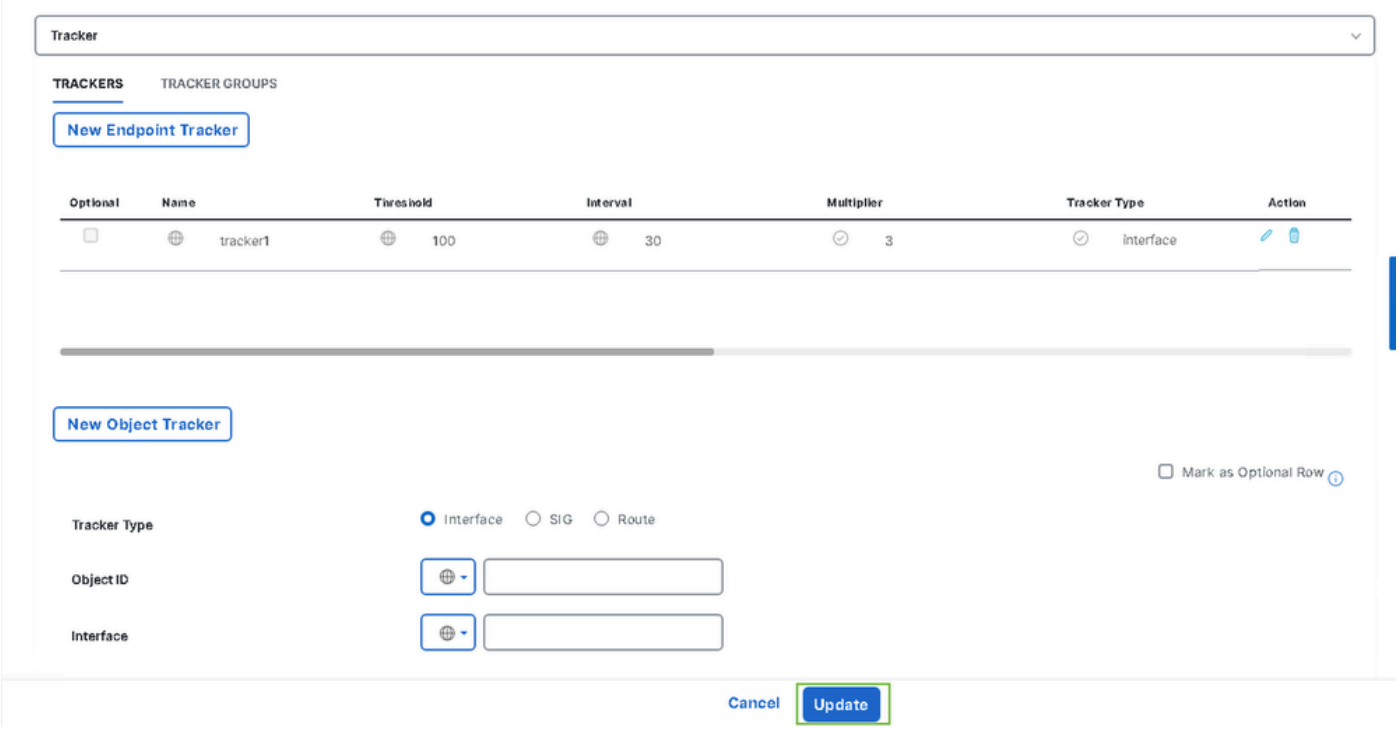
终端DNS名称：终端的DNS名称。这是Internet中的目标，路由器将探测功能发送到该目标，以确

定传输接口的状态。

单击下拉列表，然后选择全局以更改任何默认值。

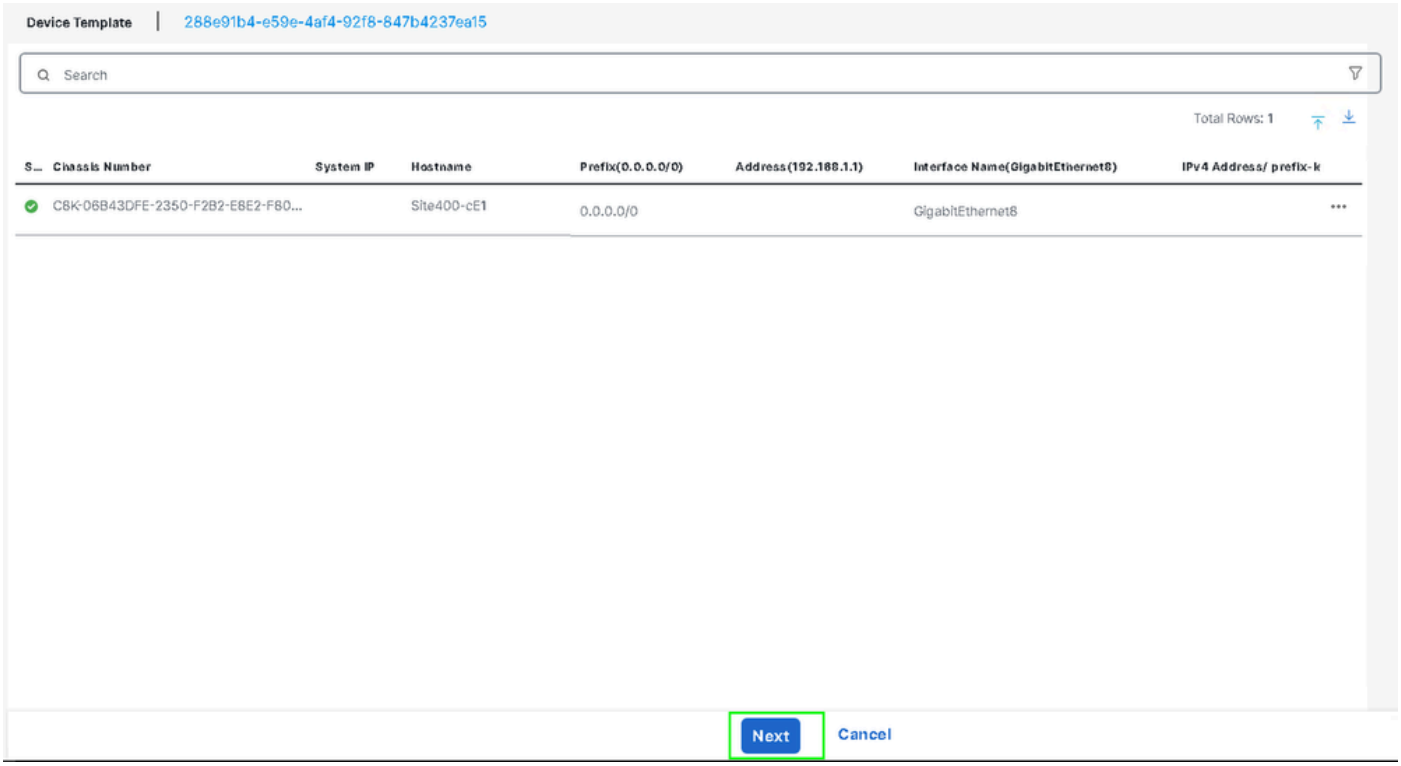


单击更新。

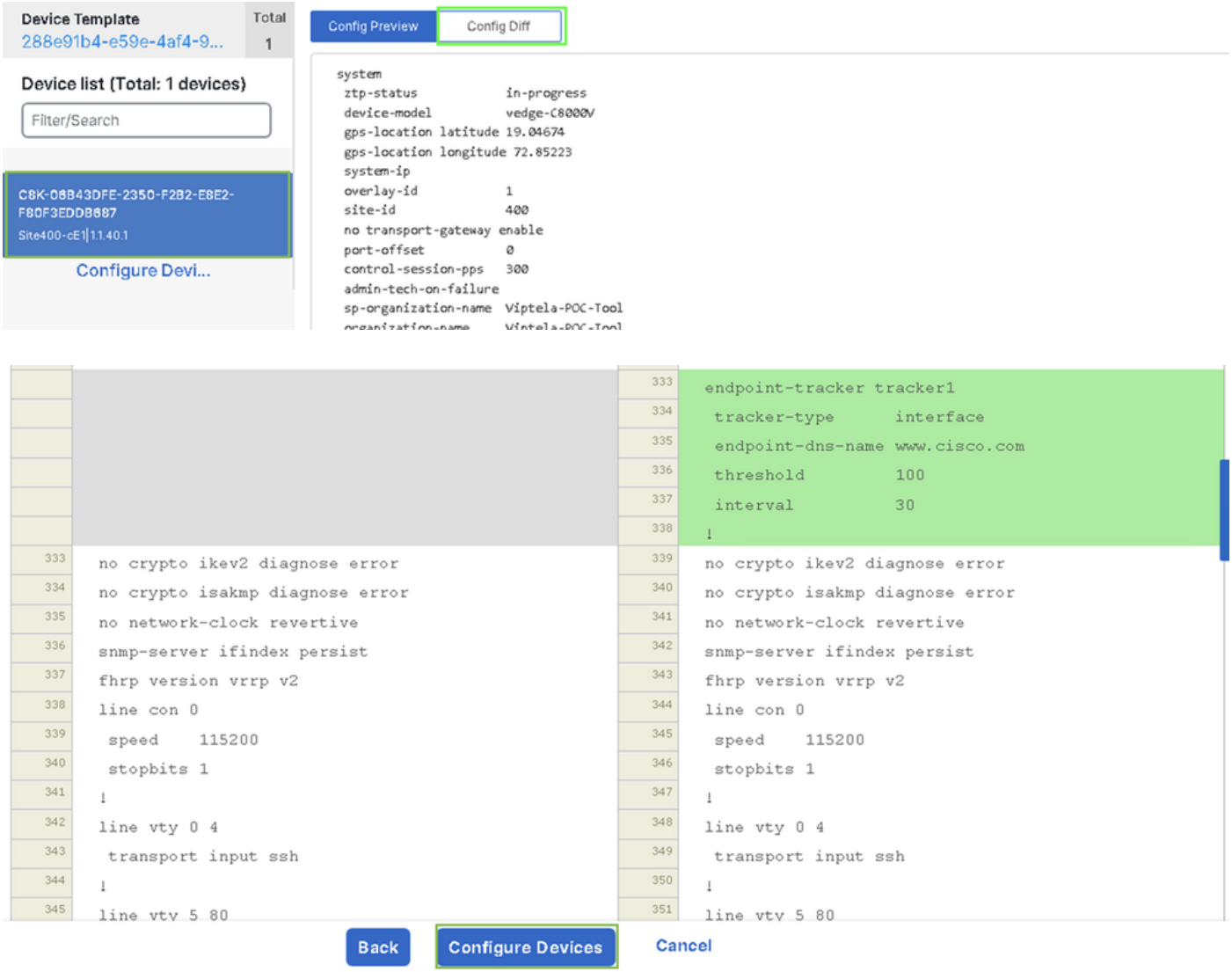


注意:确保在配置跟踪器组之前已配置两个单终端跟踪器。

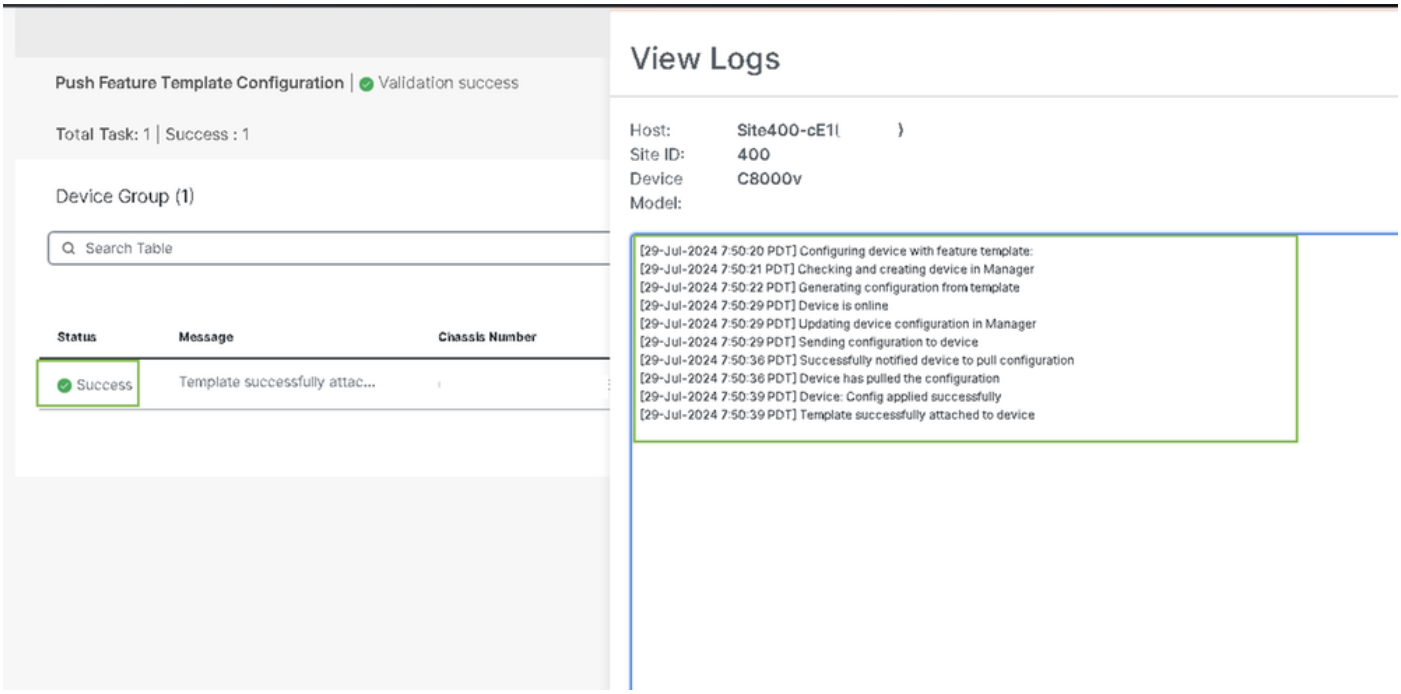
单击 Next。



单击devices，并确保配置正确。单击Config Diff和Side by Diff。点击配置设备。

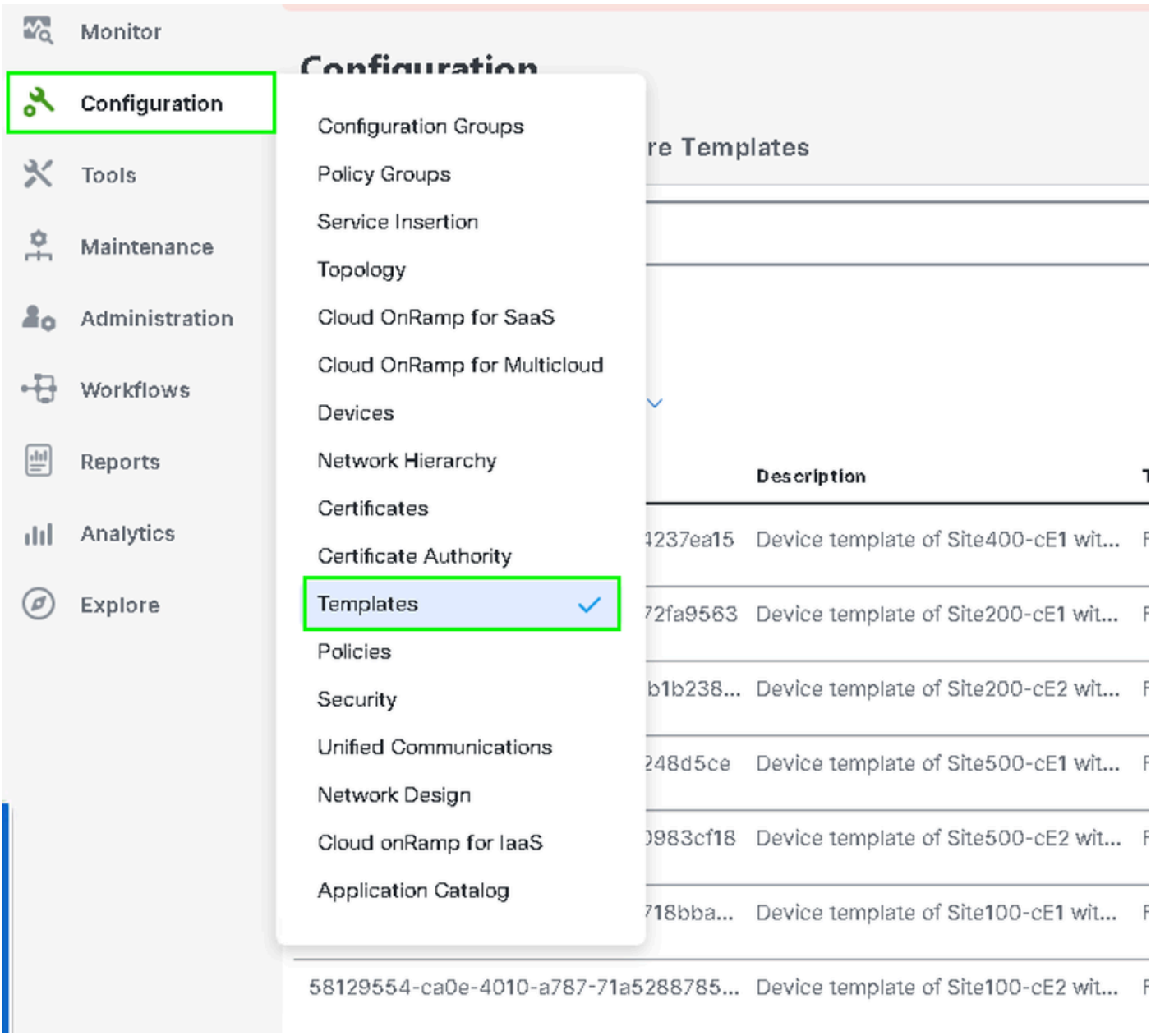


vManage已使用跟踪器配置成功配置设备模板。

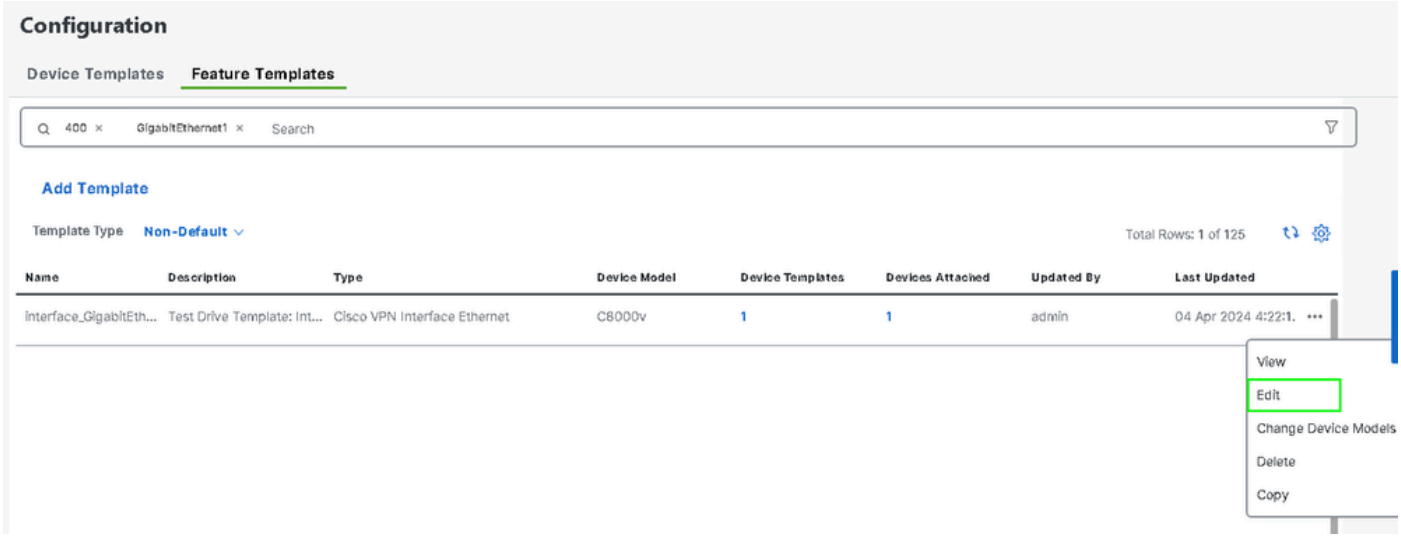


步骤2.将跟踪器绑定到传输接口

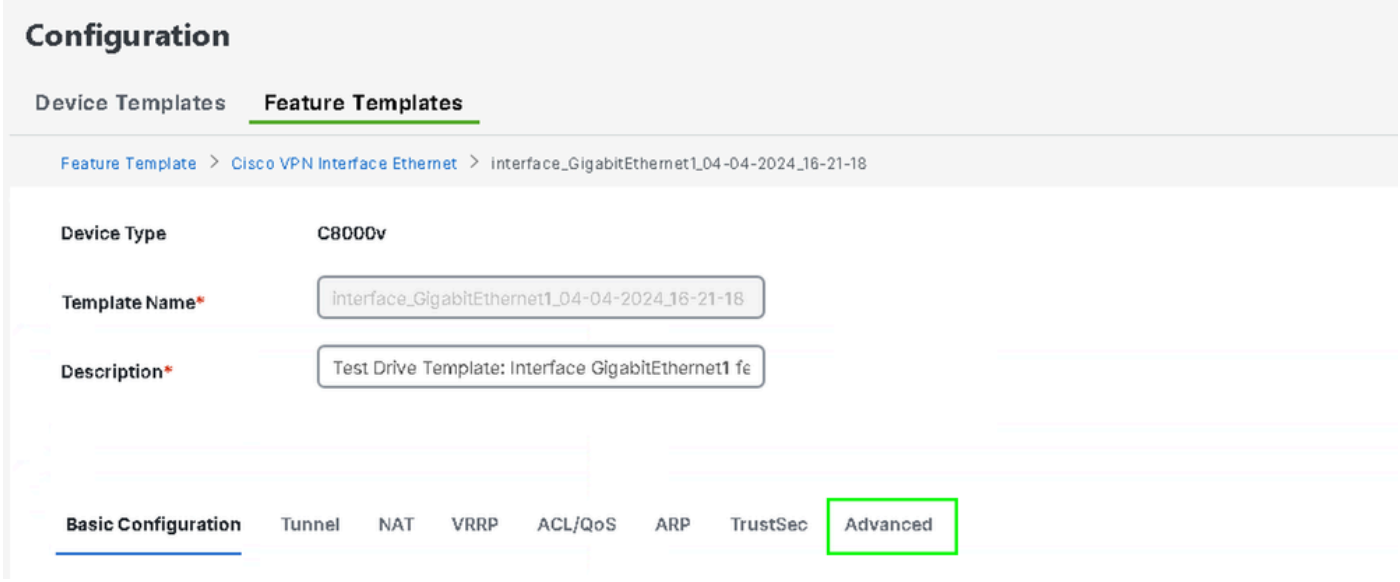
在Cisco SD-WAN Manager菜单中，导航到Configuration > Templates。



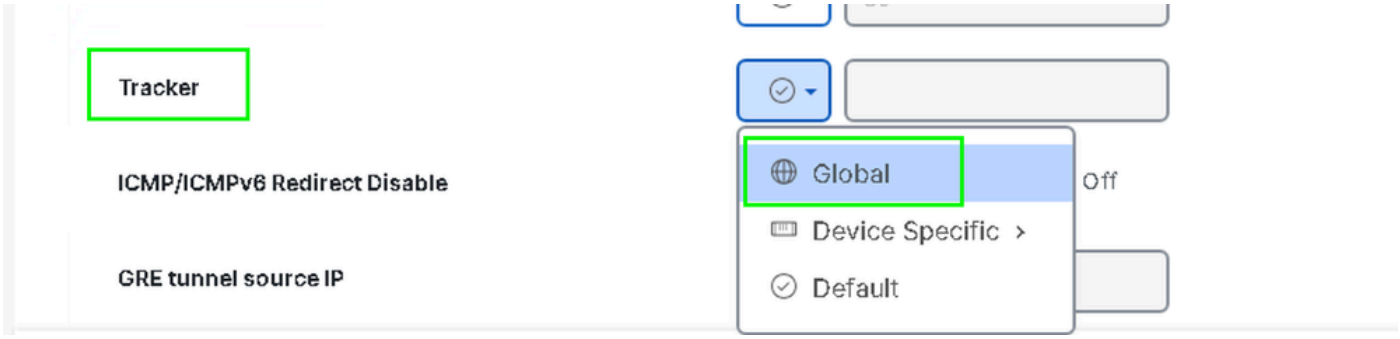
在搜索栏中搜索NAT Transport Interface功能模板，单击三个点(...)，然后单击Edit进行修改。



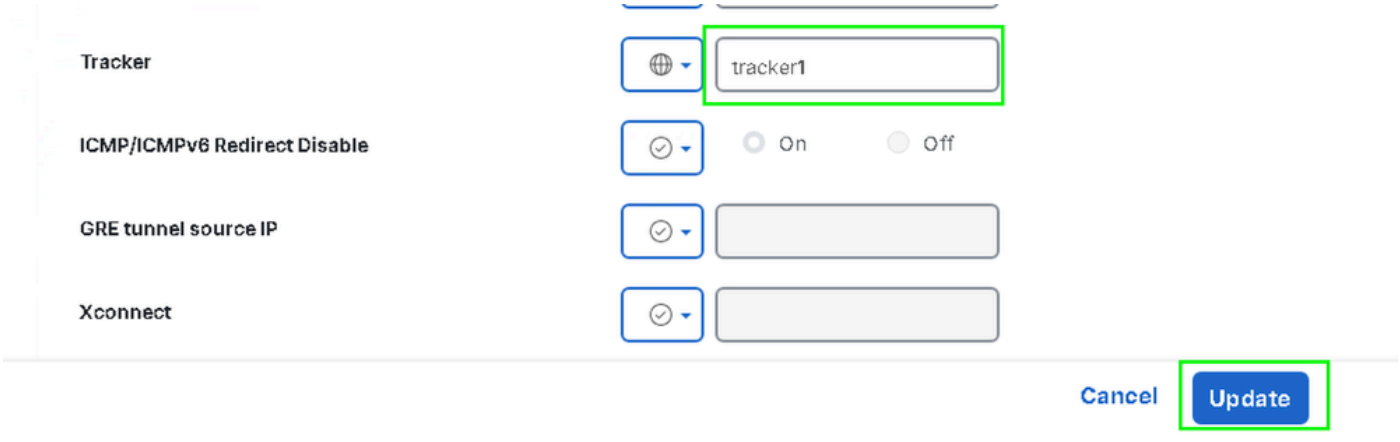
单击 Advanced 选项卡。



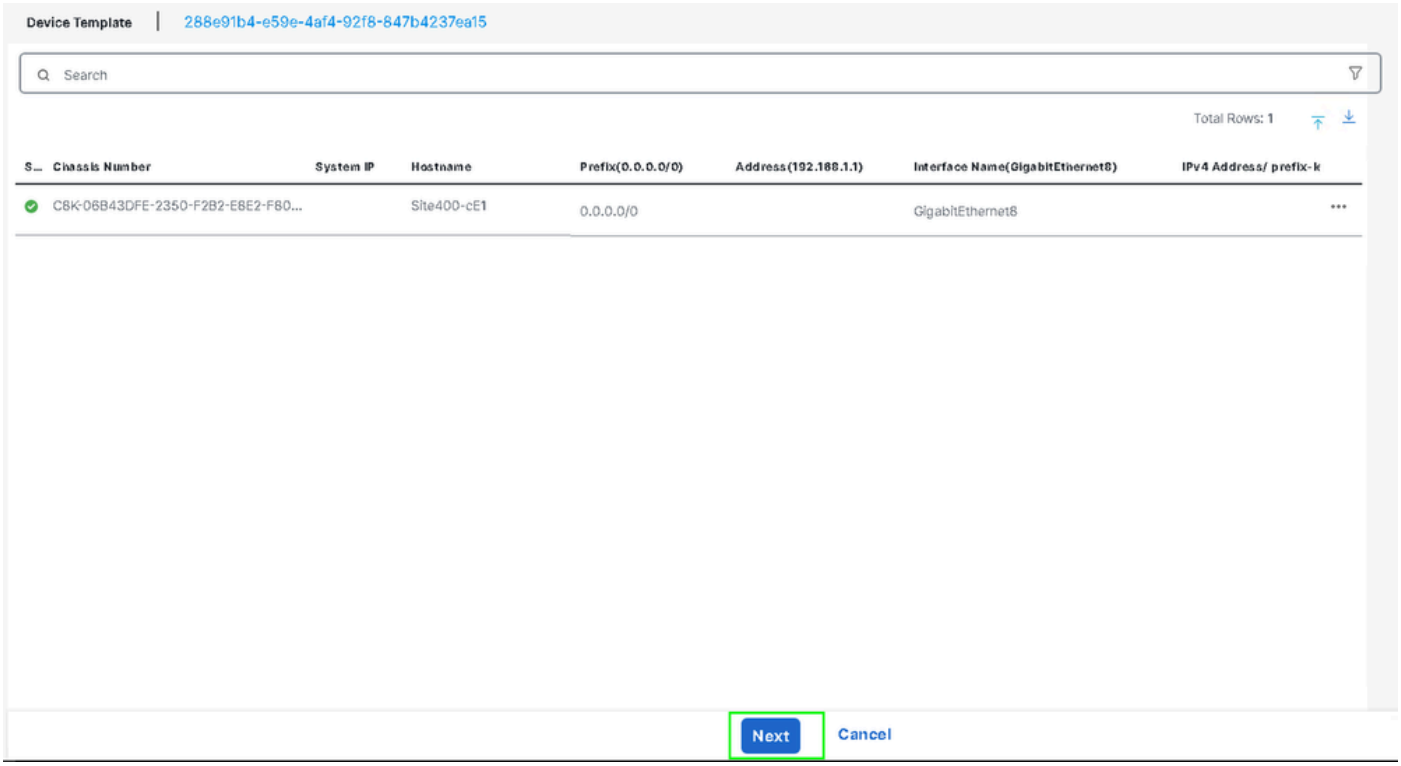
要在跟踪器上添加跟踪器名称，请从下拉菜单中选择Global。



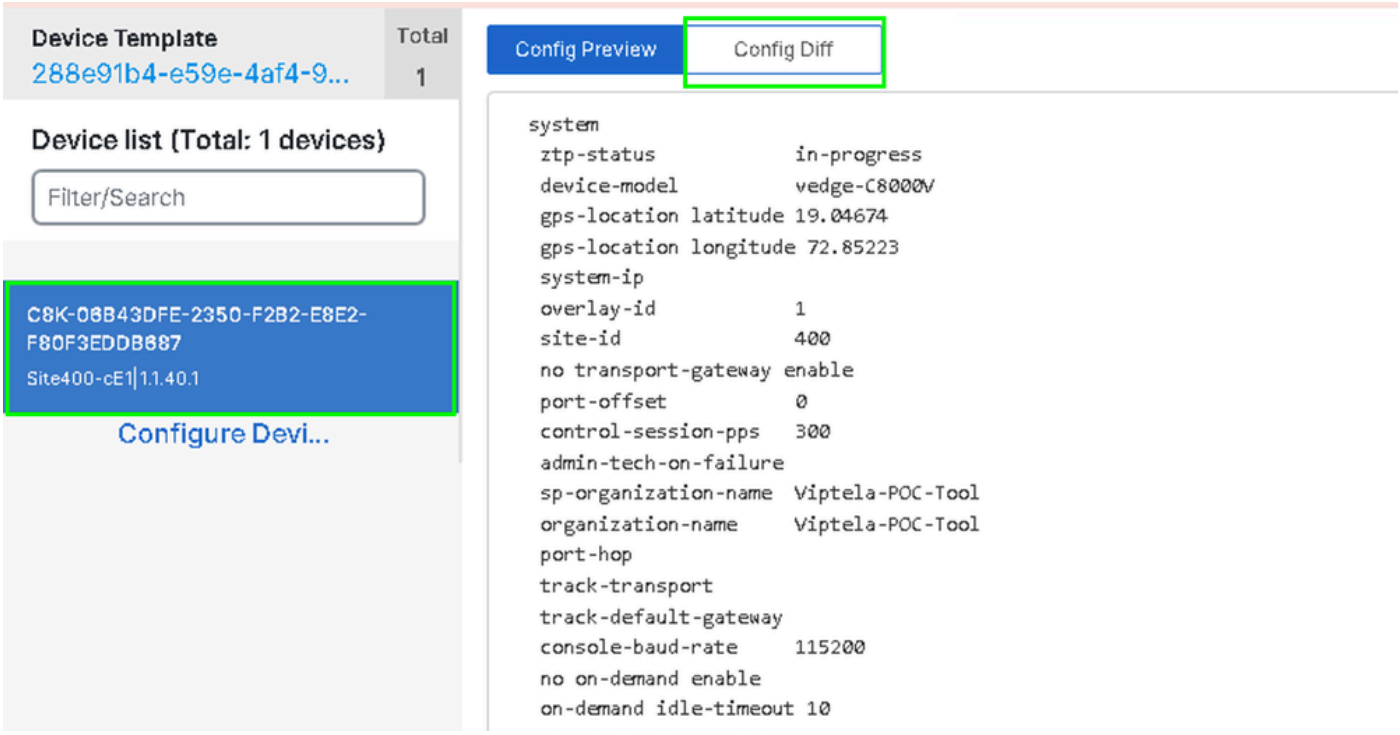
输入在系统模板中创建的跟踪器名称，然后单击Update。

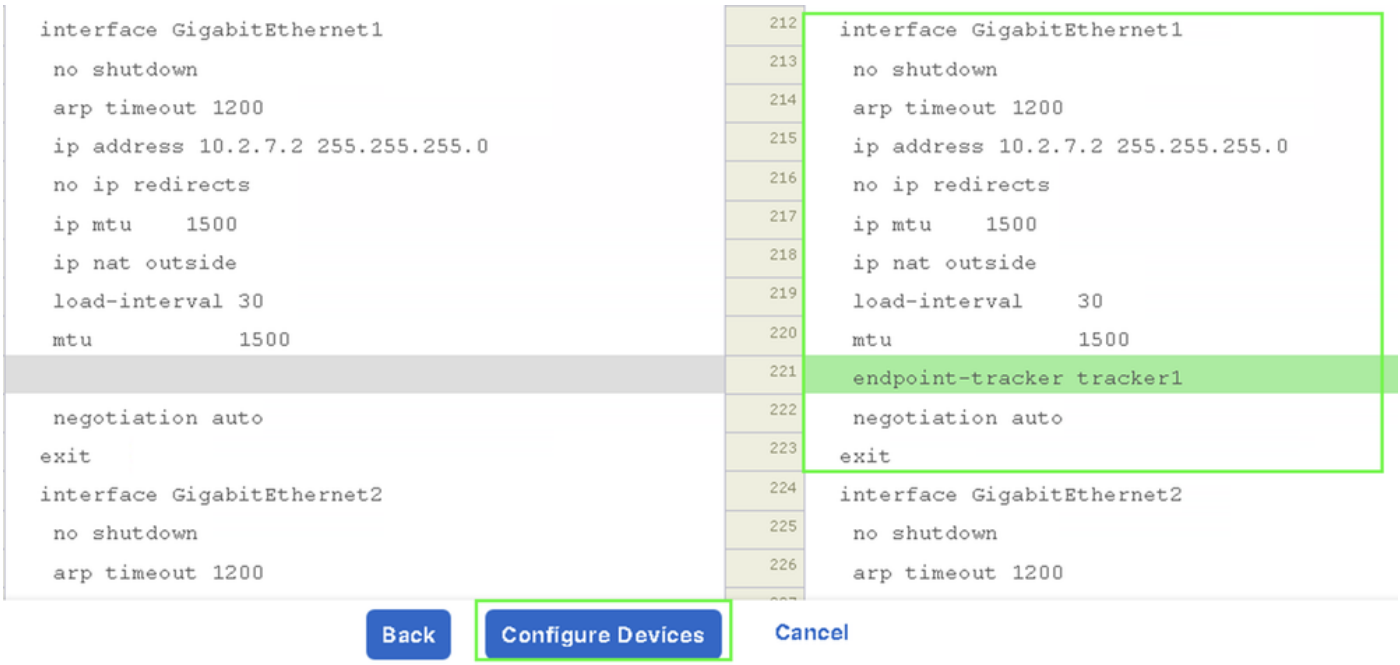


单击 Next。

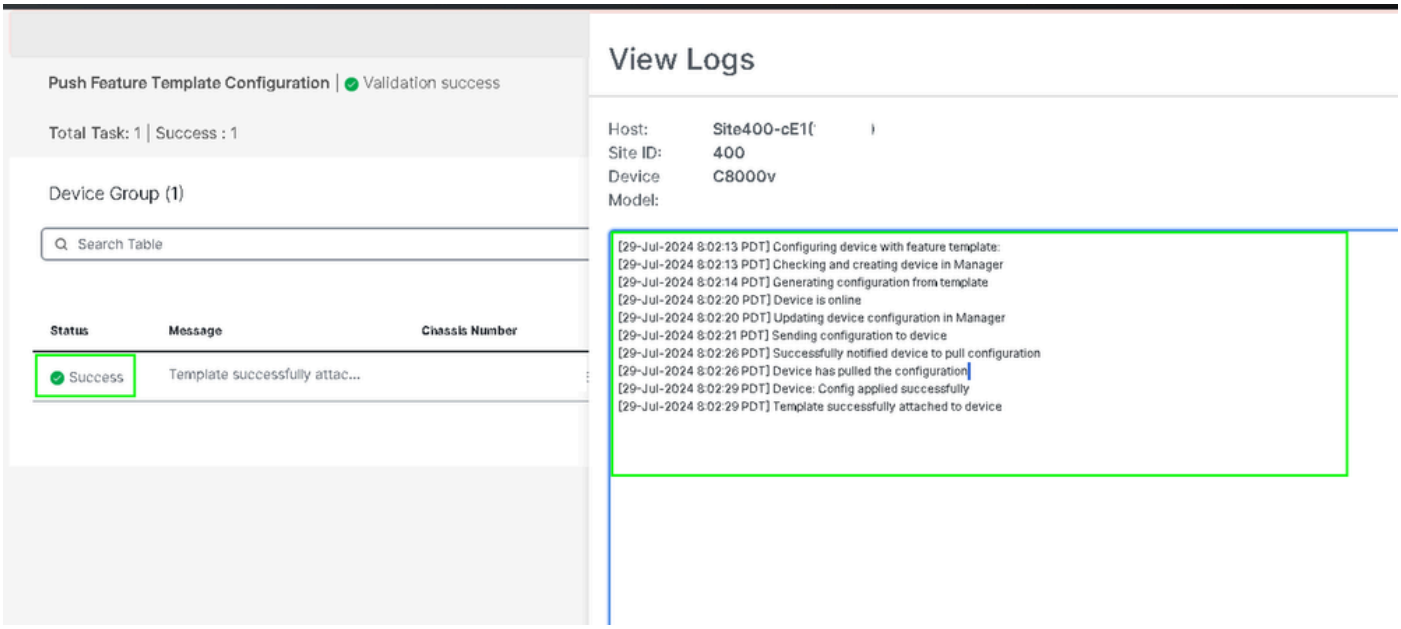


单击devices，并确保配置正确。单击Config Diff和Side by Diff。点击配置设备。





vManage已成功配置设备模板。

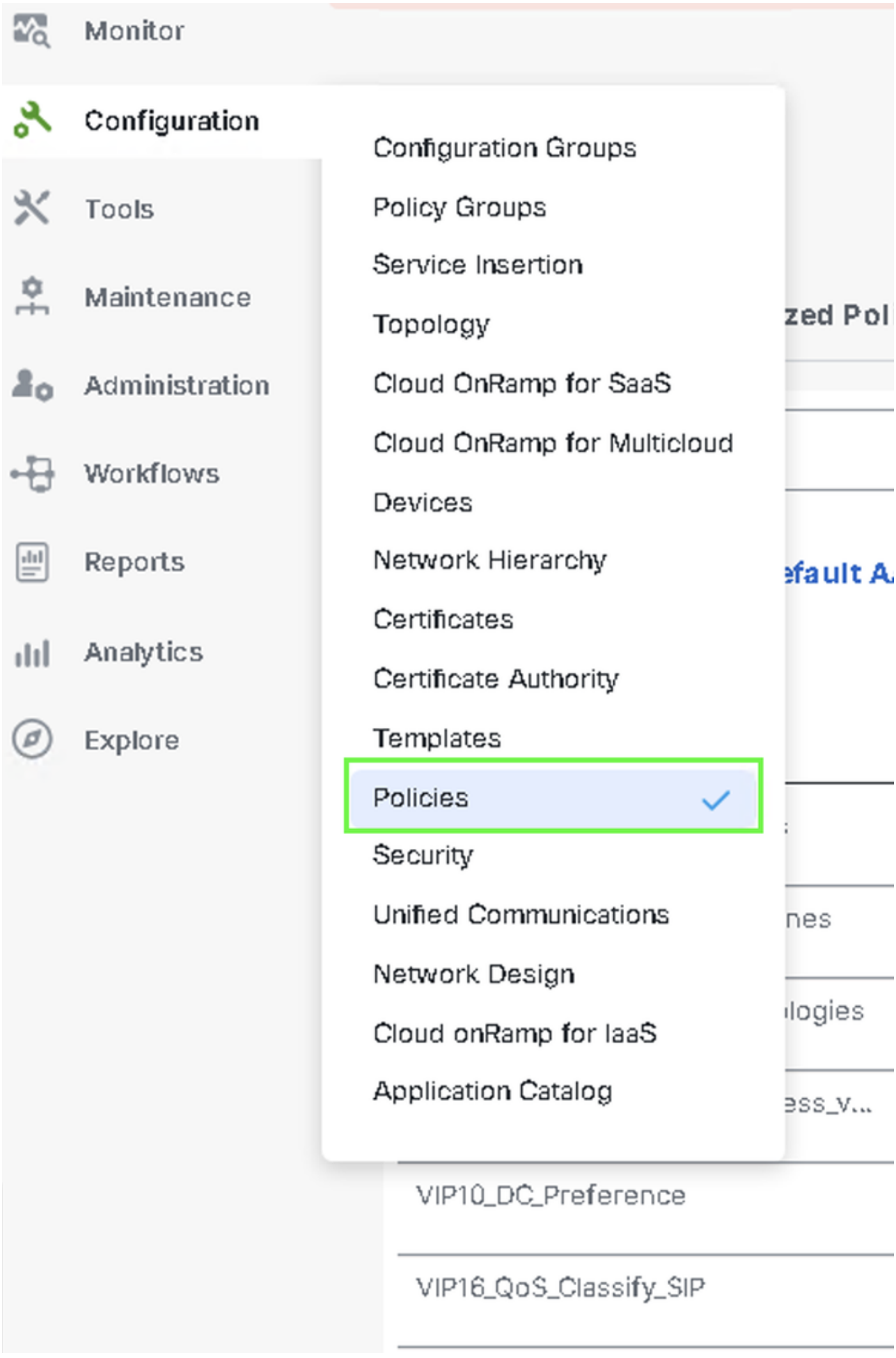


步骤3.在现有DIA策略上启用NAT回退

Cisco IOS XE Catalyst SD-WAN设备支持直接互联网接入(DIA)的NAT回退功能。NAT回退功能允许在主NAT路径失败时流量使用备用路径。即使主NAT配置存在问题，这也可确保持续连接。

要使用Cisco SD-WAN Manager启用NAT回退：

从Cisco SD-WAN Manager菜单，导航到配置>策略。


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
```

输出显示如何使用show endpoint-tracker和show endpoint-tracker GigabitEthernet1命令验证跟踪器状态。

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

输出显示有关跟踪器的计时器相关信息，以帮助调试与跟踪器相关的问题（如果有）：

```
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
```

show ip sla summary命令的输出。

```
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   Last
                          Code     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
```

使用show sdwan policy from-vsmart命令验证设备上应用的回退配置。

<#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
```

故障排除跟踪器

在边缘设备上启用这些调试，以检查路由器如何发送探测来确定传输接口的状态。

- 要监控路由器如何发送探测并确定传输接口的状态，请使用debug platform software sdwan tracker命令，该命令在17.12.x版本之前一直受支持。
- 从17.13.x开始，要监控探测日志，请启用这些调试。
  - set platform software trace ios R0 sdwanrp-tracker debug
  - set platform software trace ios R0 sdwanrp-cfg debug

- 要检查与IP SLA操作错误和跟踪相关的日志，请启用这些调试。这些日志显示IP SLA操作是否失败。
  - debug ip sla trace
  - debug ip sla error

运行以下show和monitor命令以检查调试日志：

- show logging profile sdwan internal
- 监控日志记录配置文件sdwan internal

```
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 Sta
2024/08/13 08:02:28.409197024 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 Que
2024/08/13 08:02:28.409215496 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 DNS
2024/08/13 08:02:28.409242243 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 Sou
2024/08/13 08:02:28.409274690 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 Des
2024/08/13 08:02:28.409298157 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 Sou
2024/08/13 08:02:28.409377223 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 Nex
2024/08/13 08:02:28.409391034 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 Rea
2024/08/13 08:02:28.409434969 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 act
2024/08/13 08:02:28.409525831 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 Pro
2024/08/13 08:02:28.426966448 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 Que
2024/08/13 08:02:28.427004143 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 Rec
2024/08/13 08:02:28.427029754 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 RTT
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 IPS
2024/08/13 08:02:28.427219960 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common Sta
2024/08/13 08:02:28.427238042 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common Sta
2024/08/13 08:02:28.427301952 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common Sta
2024/08/13 08:02:28.427316275 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common Sta
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 TRU
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 Sta
2024/08/13 08:02:28.427370416 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common Sta
2024/08/13 08:02:28.427555382 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common Sta
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 Sta
2024/08/13 08:02:28.427588947 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common Sta
2024/08/13 08:02:28.427600567 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common Sta
2024/08/13 08:02:28.427611465 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common Sta
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 sla
2024/08/13 08:02:55.599966240 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:3 Sta
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 Next
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
```

相关信息

为SD-WAN实施直接互联网接入(DIA)

Cisco Catalyst SD-WAN NAT配置指南

Cisco IOS XE Catalyst SD-WAN设备上的NAT回退

技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。