Configuración de OnRamp de nube SD-WAN para SaaS

Contenido

- Introducción
- Prerequisites
  - Requirements
  - Componentes Utilizados
- Antecedentes
- Configurar
  - Diagrama de la red
  - Configuraciones
    - Habilitar NAT en la interfaz de transporte
    - Crear una política AAR centralizada
    - Habilitar el acceso directo a Internet y a aplicaciones en vManage
- Verificación
- Información Relacionada

Introducción

Este documento describe la configuración de Cloud OnRamp for Software as a Service (SaaS) mediante la salida local de la sucursal.

Prerequisites

Requirements

Cisco recomienda que conozca la red de área extensa definida por software (SD-WAN) de Cisco.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco vManage versión 20.9.4
- Router Cisco WAN Edge versión 17.9.3a

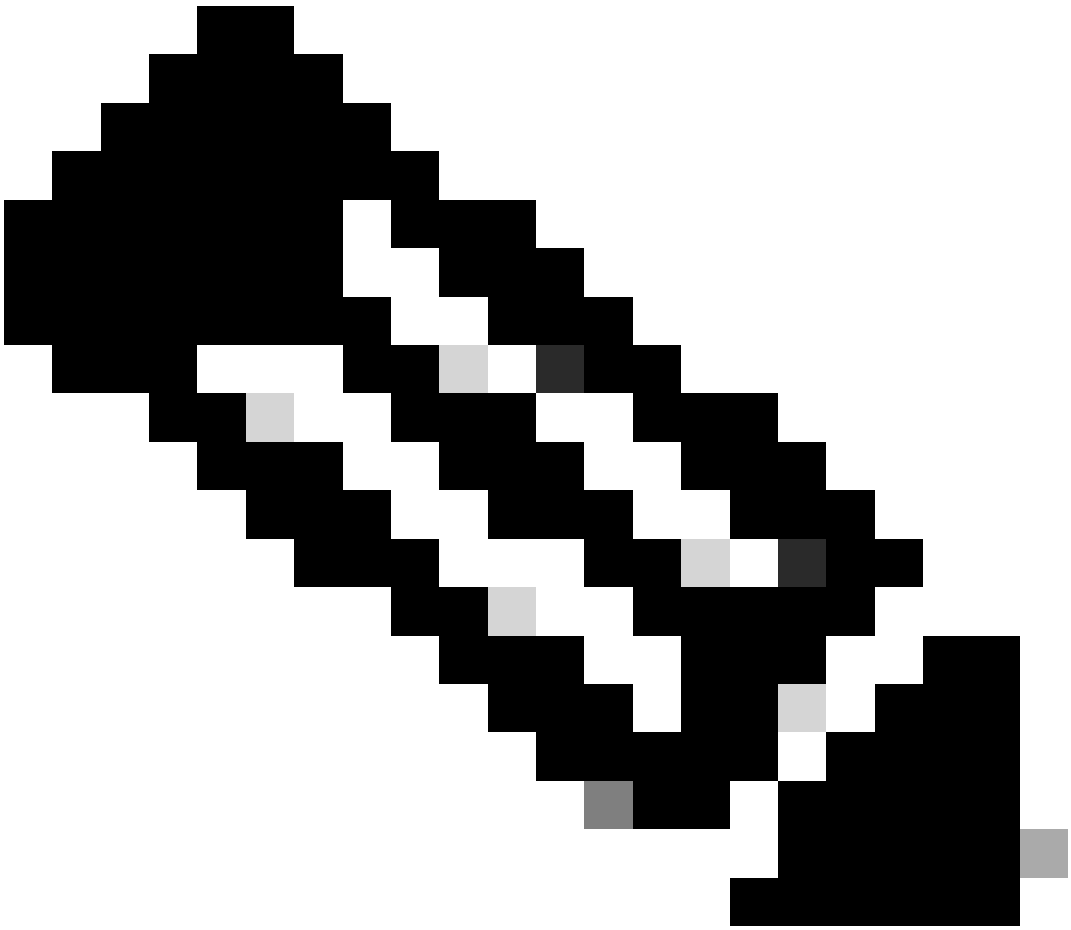
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Para una organización que utiliza SD-WAN, una sucursal suele enrutar el tráfico de aplicaciones SaaS de forma predeterminada a través de enlaces SD-WAN superpuestos a un Data Center. Desde el Data Center, el tráfico SaaS llega al servidor SaaS.

Por ejemplo, en una organización de gran tamaño con un Data Center central y sucursales, los empleados pueden utilizar Office 365 en una sucursal. De forma predeterminada, el tráfico de Office 365 en una sucursal se enruta a través de un enlace SD-WAN superpuesto a un Data Center centralizado y, desde la salida DIA, al servidor en la nube de Office 365.

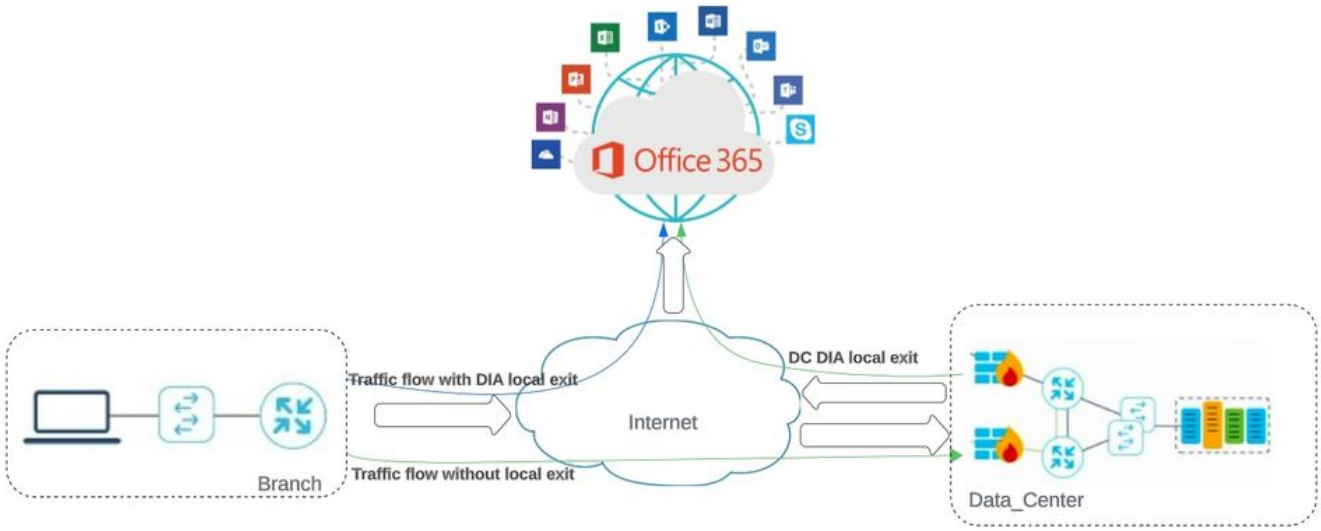
En este documento se describe esta situación: si la sucursal dispone de una conexión de acceso directo a Internet (DIA), puede mejorar el rendimiento enrutando el tráfico SaaS a través del DIA local, omitiendo el Data Center.



Nota: no se admite la configuración de Cloud OnRamp para SaaS cuando un sitio utiliza un bucle invertido como interfaz de ubicación de transporte (TLOC).

Configurar

Diagrama de la red

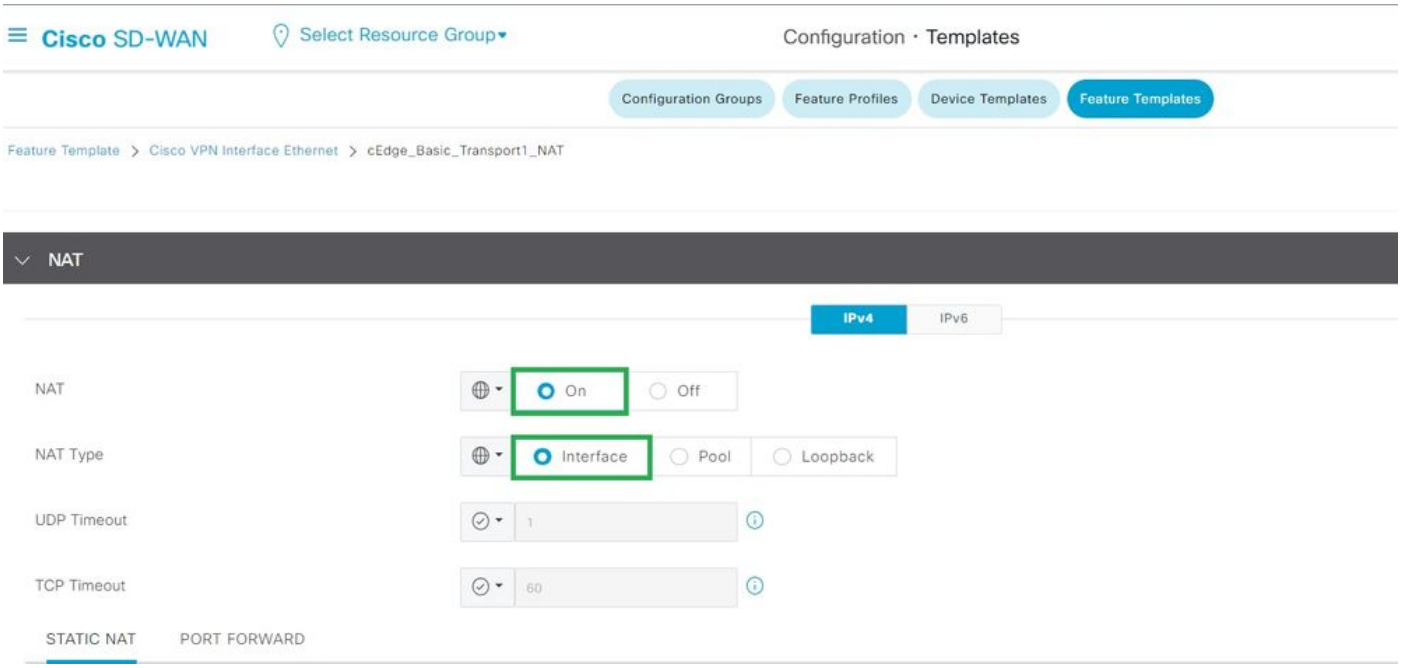


Topología de red

Configuraciones

Habilitar NAT en la interfaz de transporte

Desplácese hasta Feature Template . Elija la **Transport VPN interface** plantilla y **active NAT**.



Activar NAT de interfaz

Configuración equivalente de CLI:

```
interface GigabitEthernet2
ip nat outside

ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet2 overload
ip nat translation tcp-timeout 3600
ip nat translation udp-timeout 60
```

Crear una política AAR centralizada

Para establecer una política centralizada, debe seguir este procedimiento:

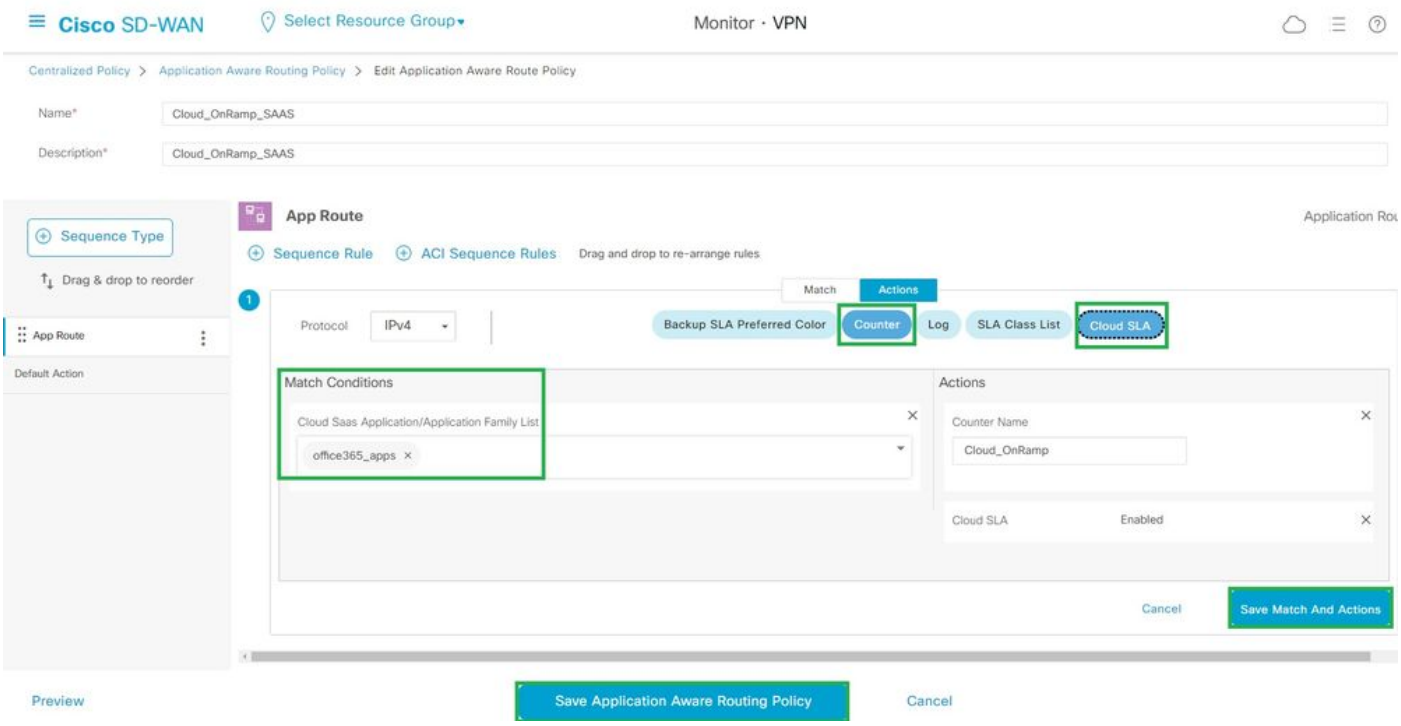
Paso 1. Crear una lista de sitios:

Plantilla NAT de interfaz VPN

Paso 2. Crear una lista de VPN:

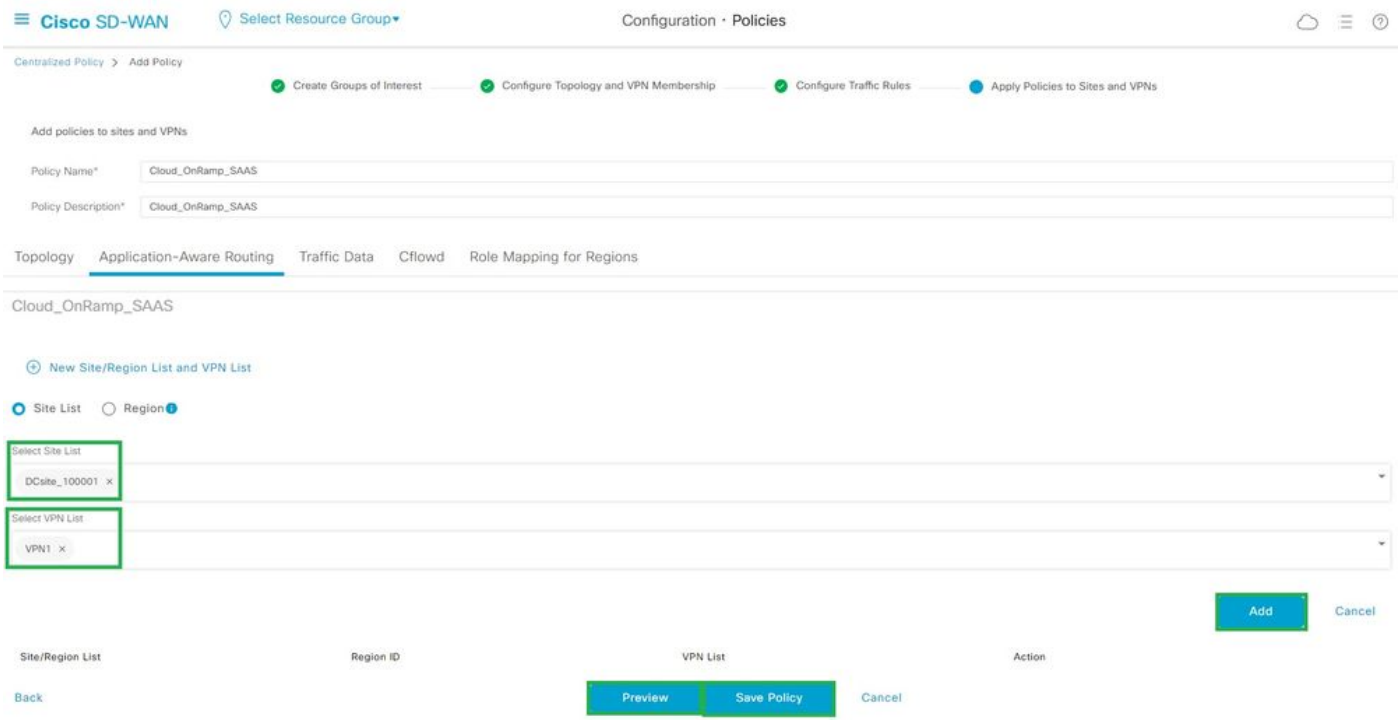
Lista de sitios personalizados de política centralizada

Paso 3. Configure el Traffic Rules y cree el Application Aware Routing Policy.



Política de ruta con reconocimiento de aplicaciones

Paso 4. Agregue la política a la dirección deseadaSites y VPN:



Agregar políticas a sitios y VPN

Política equivalente de CLI:

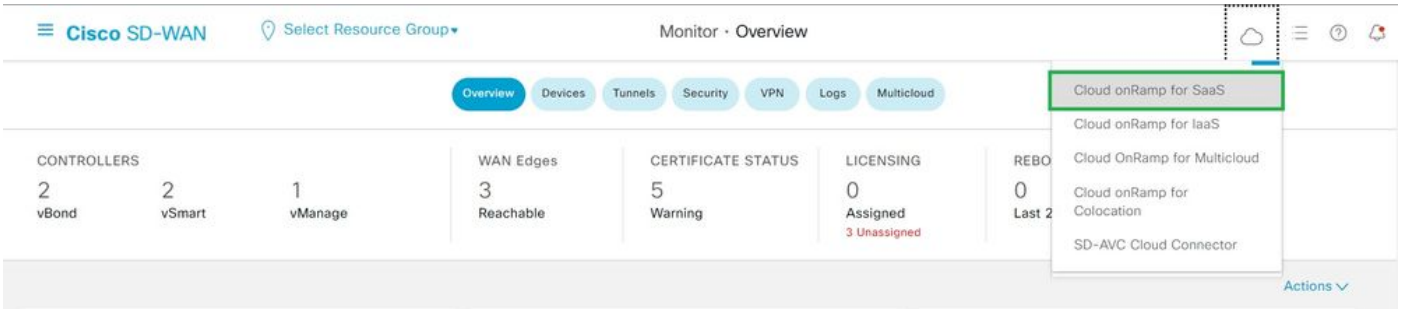
```
viptela-policy:policy
app-route-policy _VPN1_Cloud_OnRamp_SAAS
vpn-list VPN1
sequence 1
```

match
cloud-saas-app-list office365_apps
source-ip 0.0.0.0/0
!
action
count Cloud_OnRamp_-92622761
!
!
!
lists
app-list office365_apps
app skype
app ms_communicator
app windows_marketplace
app livemail_mobile
app word_online
app excel_online
app onedrive
app yammer
app sharepoint
app ms-office-365
app hockeyapp
app live_hotmail
app live_storage
app outlook-web-service
app skydrive
app ms_teams
app skydrive_login
app sharepoint_admin
app ms-office-web-apps
app ms-teams-audio
app share-point
app powerpoint_online
app ms-lync-video
app live_mesh
app ms-lync-control
app groove
app ms-live-accounts
app office_docs
app owa
app ms_sway
app ms-lync-audio
app live_groups
app office365
app windowslive
app ms-lync
app ms-services
app ms_translator
app microsoft
app sharepoint_blog
app ms_onenote
app ms-teams-video
app ms-update
app ms-teams-media
app ms_planner
app lync
app outlook
app sharepoint_online
app lync_online

```
app sharepoint_calendar
app ms-teams
app sharepoint_document
!
site-list DCsite_100001
site-id 100001
!
vpn-list VPN1
vpn 1
!
!
!
apply-policy
site-list DCsite_100001
app-route-policy _VPN1_Cloud_OnRamp_SAAS
!
!
```

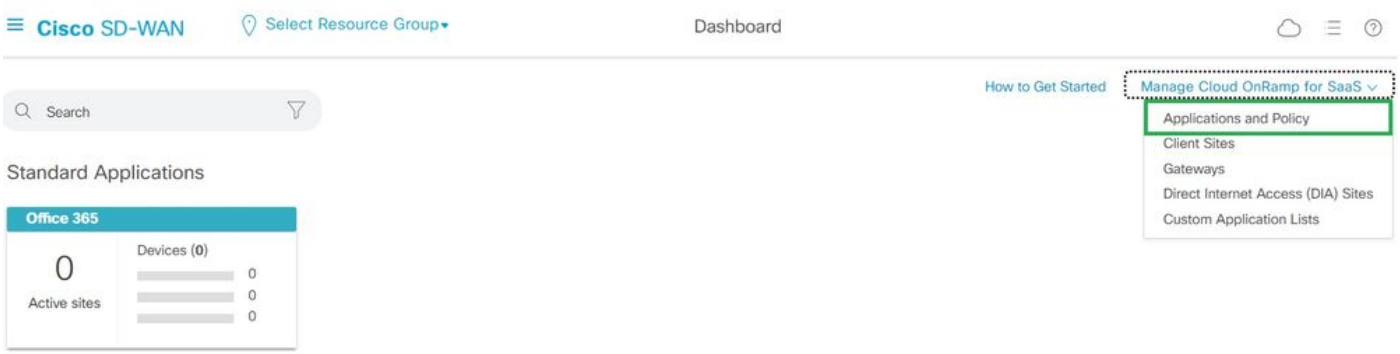
Habilitar el acceso directo a Internet y a aplicaciones en vManage

Paso 1. Desplácese hasta Cloud OnRamp for SaaS.



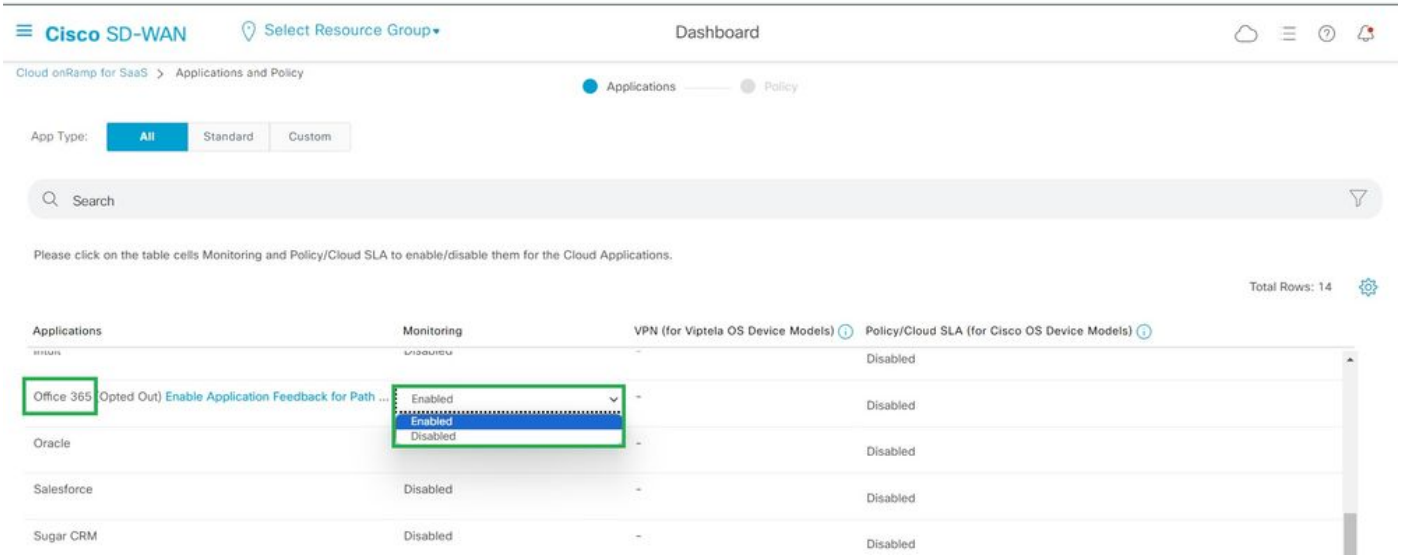
Seleccione la nube en rampa para SaaS

Paso 2. Desplácese hasta Applications and Policy.



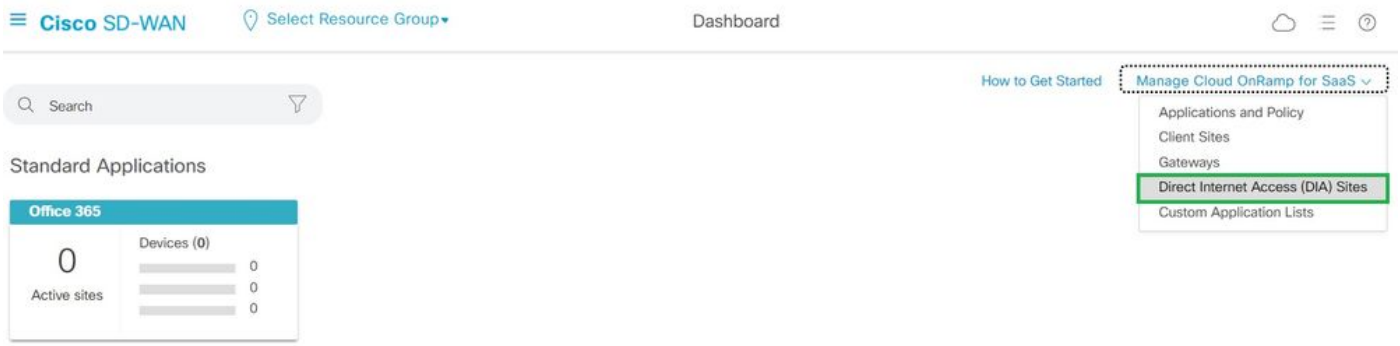
Seleccionar aplicaciones y políticas

Paso 3. Desplácese hasta Application > Enabley Save. A continuación, haga clic en Next.



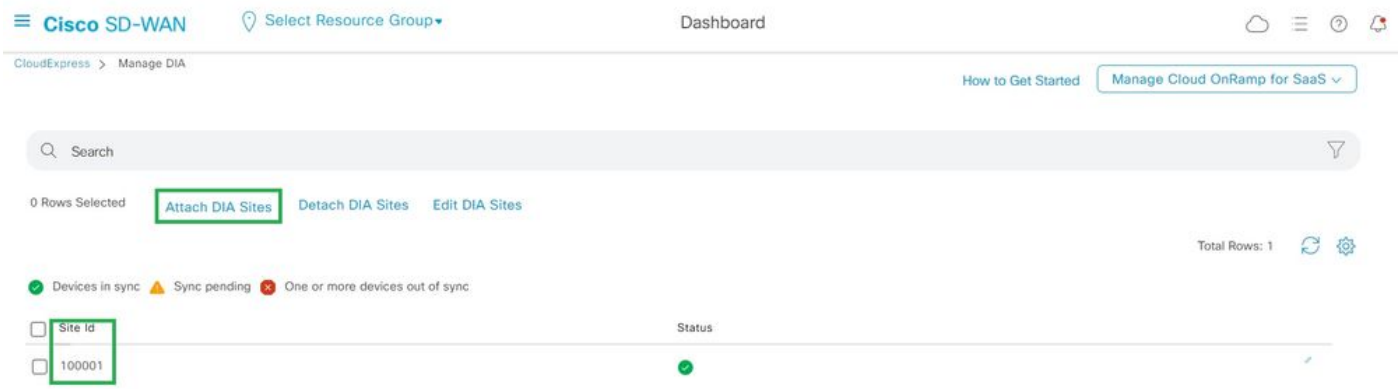
Seleccione Aplicaciones y active la supervisión

Paso 4. Desplácese hasta Direct Internet Access (DIA) Sites.



Seleccionar sitios de acceso directo a Internet

Paso 5. Desplácese hasta Attach DIA Sites y seleccione Sitios.



Adjuntar sitios DIA

Verificación

En esta sección se describen los resultados para verificar el Cloud OnRamp para SaaS.

- Esta salida muestra las salidas locales de Cloudexpress:

```
cEdge_West-01#sh sdwan cloudexpress local-exits
cloudexpress local-exits vpn 1 app 2 type app-group subapp 0 GigabitEthernet2
application office365
latency 6
loss 0
```

- Esta salida muestra las aplicaciones de Cloudexpress:

```
cEdge_West-01#sh sdwan cloudexpress applications
cloudexpress applications vpn 1 app 2 type app-group subapp 0
application office365
exit-type local
interface GigabitEthernet2
latency 6
loss 0
```

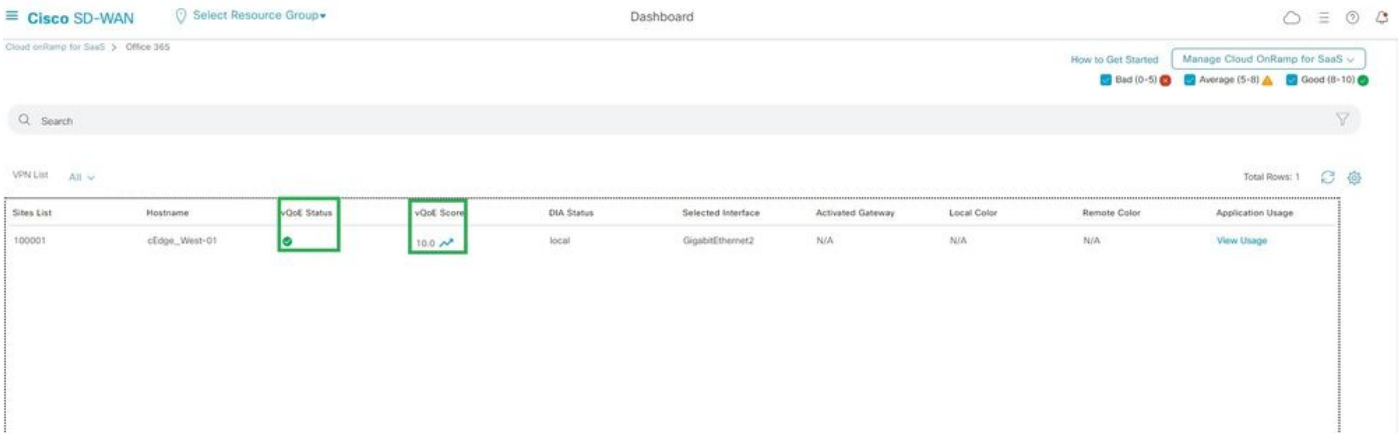
- Este resultado muestra los contadores en aumento para el tráfico interesado:

<#root>

```
cEdge_West-01#sh sdwan policy app-route-policy-filter
NAME                       NAME        COUNTER NAME                          PACKETS     BYTES
-------------------------------------------------------------------------------------------------
_VPN1_Cloud_OnRamp_SAAS    VPN1        default_action_count                  640         66303
```

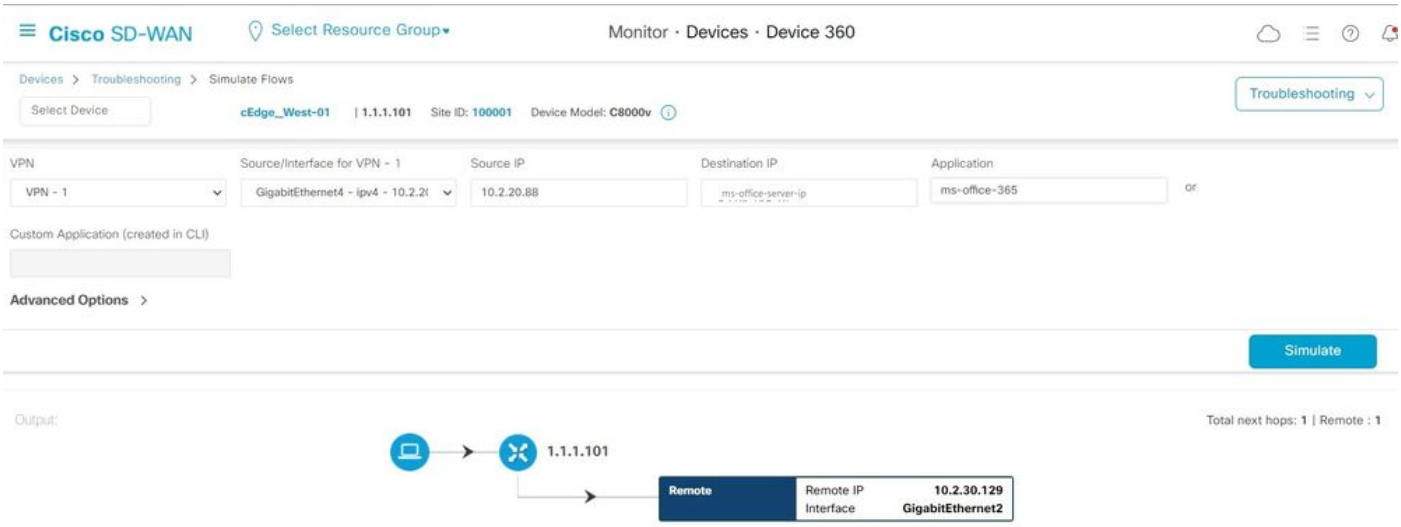
Cloud_OnRamp_-403085179 600 432292

- Este resultado muestra el estado y la puntuación de vQoE:



Estado y puntuación de vQoE

- Este resultado muestra la ruta de servicio de la GUI de vManage:



Ruta de servicio

- Este resultado muestra la trayectoria de servicio desde la CLI del dispositivo:

```
cEdge_West-01#sh sdwan policy service-path vpn 1 interface GigabitEthernet4 source-ip 10.2.20.70 dest-i
Next Hop: Remote
Remote IP: 10.2.30.129, Interface GigabitEthernet2 Index: 8
```

Información Relacionada

- Guía de configuración de Cisco Catalyst SD-WAN Cloud OnRamp
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).