

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

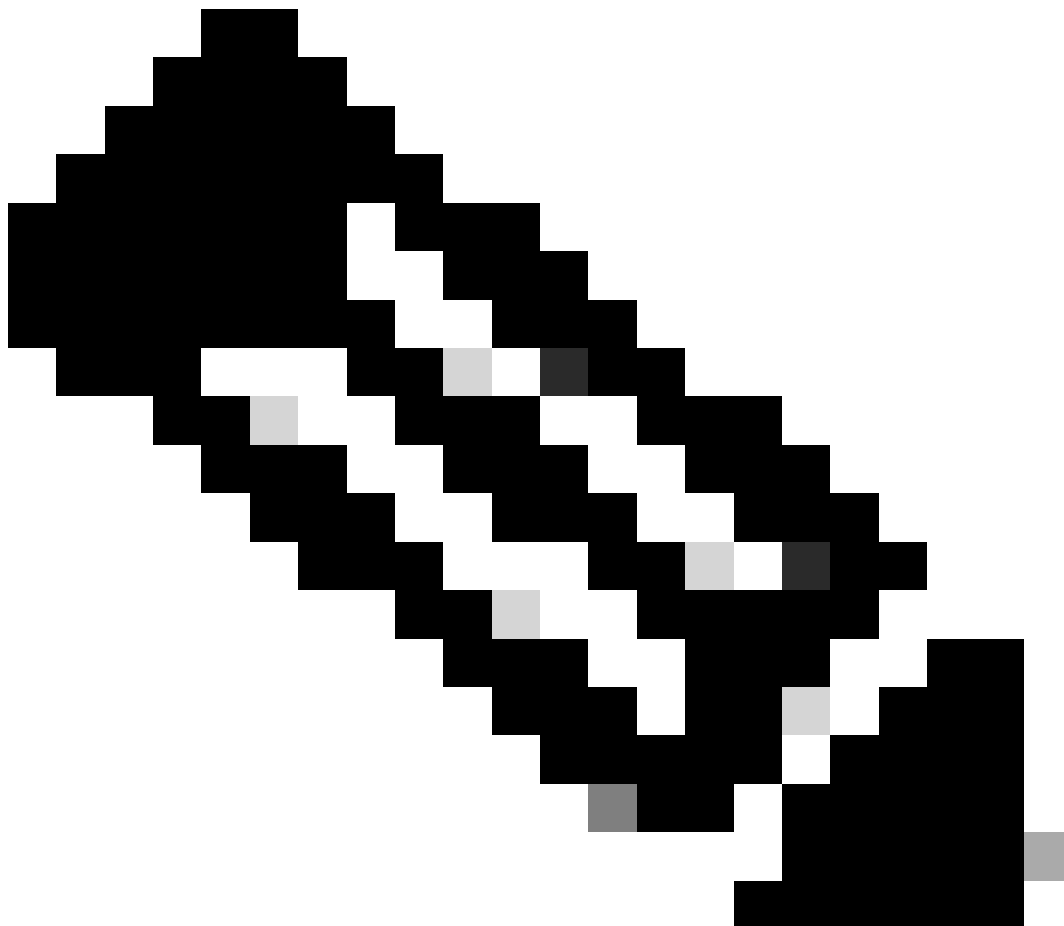
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender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

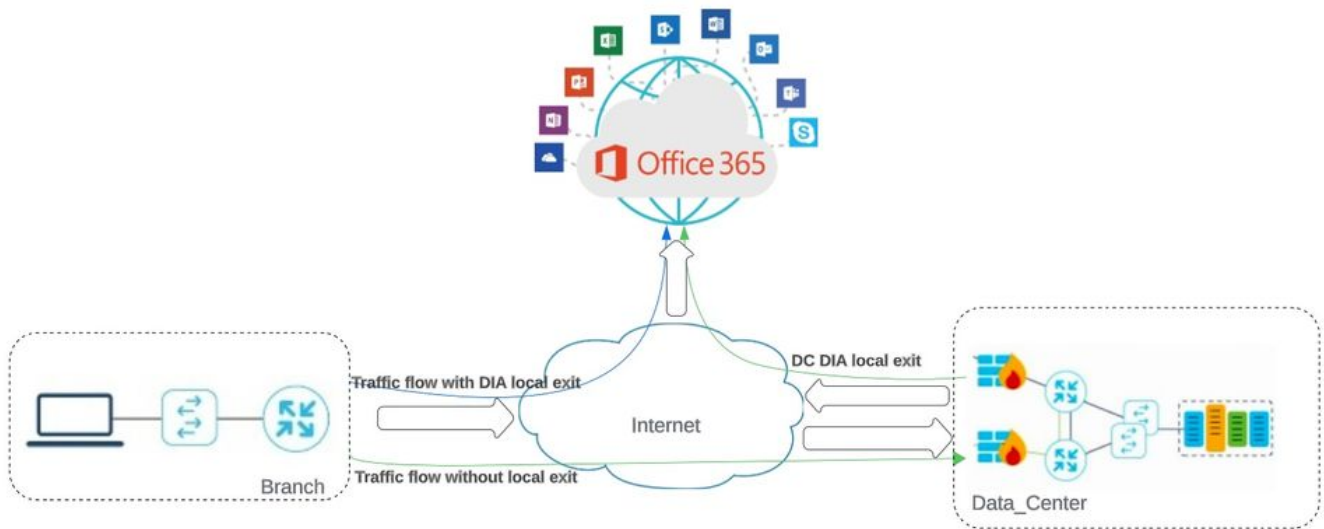
En este documento se describe esta situación: si la sucursal dispone de una conexión de acceso directo a Internet (DIA), puede mejorar el rendimiento enrutando el tráfico SaaS a través del DIA local, omitiendo el Data Center.



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**.

Cisco SD-WAN Select Resource Group Configuration · Templates

Configuration Groups Feature Profiles Device Templates **Feature Templates**

Feature Template > Cisco VPN Interface Ethernet > cEdge_Basic_Transport1_NAT

NAT

IPv4 IPv6

NAT On Off

NAT Type Interface Pool Loopback

UDP Timeout

TCP Timeout

STATIC NAT PORT FORWARD

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:

Centralized Policy > Define Lists

Select a list type on the left and start creating your groups of interest

Application
Color
Community
Data Prefix
Policer
Prefix
Site

+ New Site List

Name	Entries	Reference Count	Updated By	Last Updated	Action
DCsite_100001	100001	3	admin	11 Sep 2023 12:46:54 PM P...	

Plantilla NAT de interfaz VPN

Paso 2. Crear una lista de VPN:

Centralized Policy > Define Lists

Select a list type on the left and start creating your groups of interest

Application
Color
Community
Data Prefix
Policer
Prefix
Site

+ New Site List

Name	Entries	Reference Count	Updated By	Last Updated	Action
DCsite_100001	100001	3	admin	11 Sep 2023 12:46:54 PM P...	

Lista de sitios personalizados de política centralizada

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

Cisco SD-WAN Monitor · VPN

Centralized Policy > Application Aware Routing Policy > Edit Application Aware Route Policy

Name* Cloud_OnRamp_SAAS
Description* Cloud_OnRamp_SAAS

App Route Application Router

Sequence Type

Drag & drop to reorder

Sequence Rule ACI Sequence Rules Drag and drop to re-arrange rules

Match Actions

Backup SLA Preferred Color Counter Log SLA Class List Cloud SLA

Protocol IPv4

Match Conditions

Cloud Saas Application/Application Family List

office365_apps

Actions

Counter Name Cloud_OnRamp

Cloud SLA Enabled

Cancel Save Match And Actions

Preview Save Application Aware Routing Policy Cancel

Política de ruta con reconocimiento de aplicaciones

Paso 4. Agregue la política a la dirección deseada Sites y VPN:

Cisco SD-WAN Configuration · Policies

Centralized Policy > Add Policy

Create Groups of Interest Configure Topology and VPN Membership Configure Traffic Rules Apply Policies to Sites and VPNs

Add policies to sites and VPNs

Policy Name* Cloud_OnRamp_SAAS
Policy Description* Cloud_OnRamp_SAAS

Topology Application-Aware Routing Traffic Data Cflowd Role Mapping for Regions

Cloud_OnRamp_SAAS

New Site/Region List and VPN List

Site List Region

Select Site List

DCsite_100001

Select VPN List

VPN1

Add Cancel

Site/Region List Region ID VPN List Action

Back Preview Save Policy Cancel

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
!
!

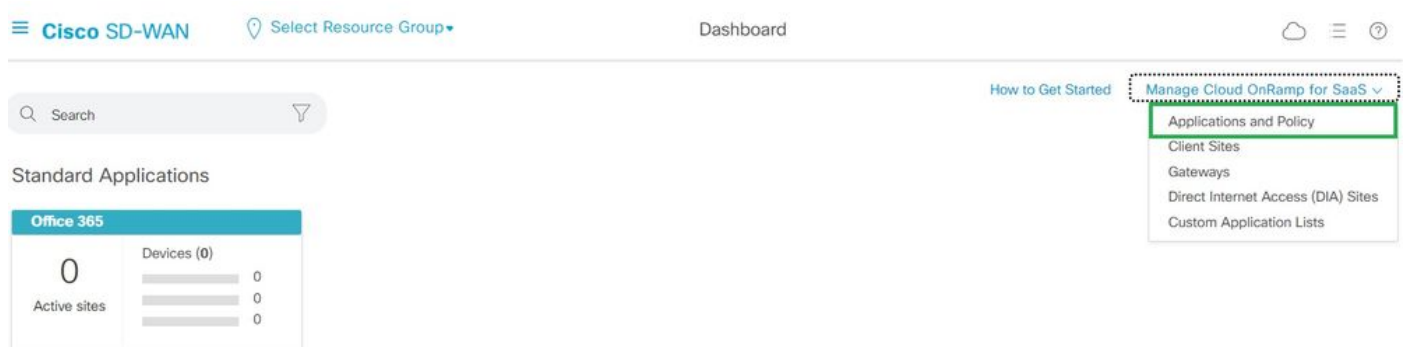
Habilitar el acceso directo a Internet y a aplicaciones en vManage

Paso 1. Desplácese hasta Cloud OnRamp for SaaS.



Selecione la nube en rampa para SaaS

Paso 2. Desplácese hasta Applications and Policy.



Seleccionar aplicaciones y políticas

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

Cisco SD-WAN Select Resource Group Dashboard

Cloud onRamp for SaaS > Applications and Policy

App Type: All Standard Custom

Search

Please click on the table cells Monitoring and Policy/Cloud SLA to enable/disable them for the Cloud Applications.

Total Rows: 14

Applications	Monitoring	VPN (for Viptela OS Device Models)	Policy/Cloud SLA (for Cisco OS Device Models)
Office 365 (Opted Out) Enable Application Feedback for Path ...	Enabled	-	Disabled
Oracle	Enabled	-	Disabled
Salesforce	Disabled	-	Disabled
Sugar CRM	Disabled	-	Disabled

Seleccione Aplicaciones y active la supervisión

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

Cisco SD-WAN Select Resource Group Dashboard

Search

Standard Applications

Office 365

0 Active sites

Devices (0)

0

0

0

How to Get Started

- Manage Cloud OnRamp for SaaS
 - Applications and Policy
 - Client Sites
 - Gateways
 - Direct Internet Access (DIA) Sites
 - Custom Application Lists

Seleccionar sitios de acceso directo a Internet

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

The screenshot shows the Cisco SD-WAN CloudExpress interface for managing Cloud OnRamp for SaaS. At the top, there is a navigation bar with 'Cisco SD-WAN', 'Select Resource Group', and 'Dashboard'. Below this, there are links for 'How to Get Started' and 'Manage Cloud OnRamp for SaaS'. A search bar is present, and below it, there are buttons for 'Attach DIA Sites', 'Detach DIA Sites', and 'Edit DIA Sites'. The main area displays a table with one row: Site Id 100001, with a green status indicator. The status bar at the bottom indicates 'Devices in sync'.

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:

The screenshot shows the Cisco SD-WAN Dashboard for Office 365. A table titled 'VPN List' displays the following data:

Sites List	Hostname	vQoE Status	vQoE Score	DIA Status	Selected Interface	Activated Gateway	Local Color	Remote Color	Application Usage
100001	cEdge_West-01	Good (8-10)	10.0	local	GigabitEthernet2	N/A	N/A	N/A	View Usage

Estado y puntuación de vQoE

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

Cisco SD-WAN | Select Resource Group | Monitor · Devices · Device 360

Devices > Troubleshooting > Simulate Flows

Select Device: **cEdge_West-01** | 1.1.1.101 | Site ID: 100001 | Device Model: C8000v

VPN: **VPN - 1** | Source/Interface for VPN - 1: **GigabitEthernet4 - ipv4 - 10.2.20.70** | Source IP: **10.2.20.88** | Destination IP: **ms-office-server-ip** | Application: **ms-office-365**

Custom Application (created in CLI):

Advanced Options >

Simulate

Output:

Total next hops: 1 | Remote : 1

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-ip 10.2.30.129
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).