Konfigurieren von SD-WAN Cloud OnRamp für SaaS

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration für Cloud OnRamp für Software as a Service (SaaS) mithilfe des lokalen Verlassens der Außenstelle beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse des Cisco Software-Defined Wide Area Network (SD-WAN) verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco vManage, Version 20.9.4
- Cisco WAN Edge-Router Version 17.9.3a

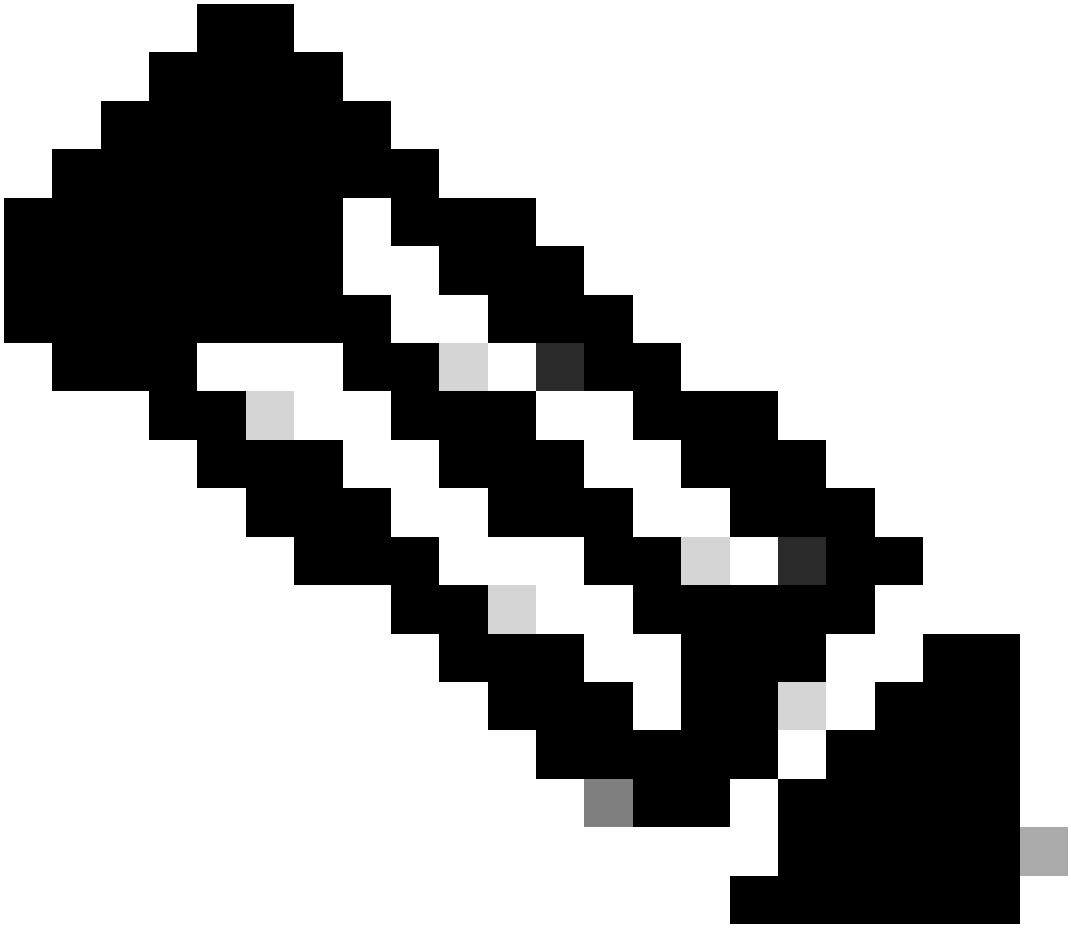
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen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

Hintergrundinformationen

Bei Unternehmen, die SD-WAN verwenden, leitet eine Außenstelle den Datenverkehr von SaaS-Anwendungen standardmäßig über SD-WAN-Overlay-Links zu einem Rechenzentrum weiter. Vom Rechenzentrum aus gelangt der SaaS-Datenverkehr zum SaaS-Server.

In großen Unternehmen mit zentralem Rechenzentrum und Zweigstellen können Mitarbeiter beispielsweise Office 365 in Zweigstellen verwenden. Standardmäßig wird der Office 365-Datenverkehr in einer Zweigstelle über eine SD-WAN-Overlay-Verbindung zu einem zentralisierten Rechenzentrum und vom DIA-Ausgang zum Office 365-Cloud-Server geleitet.

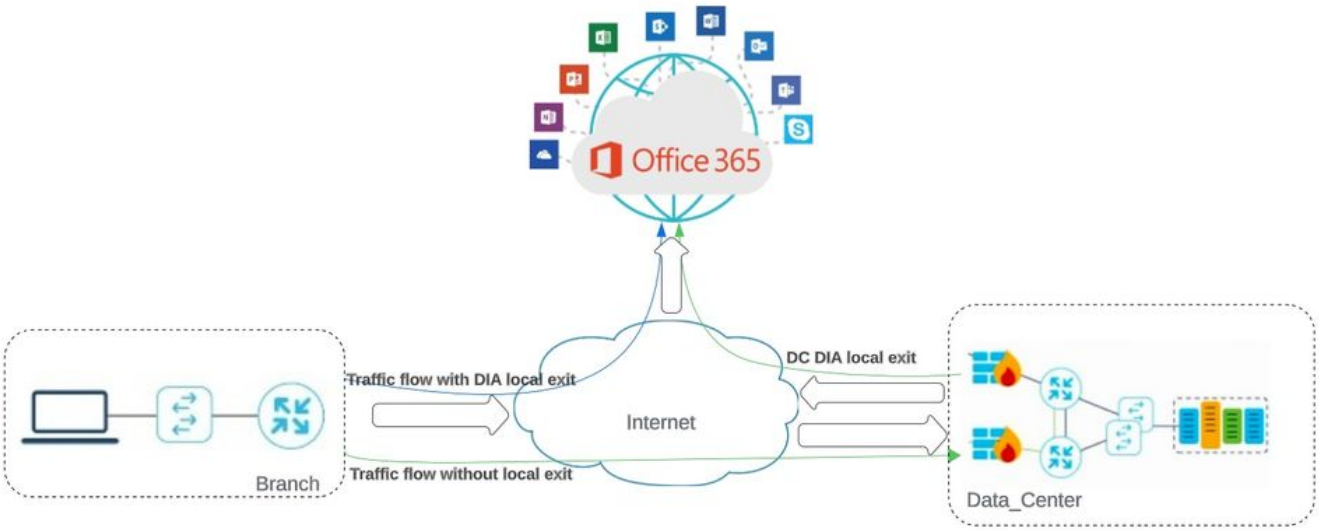
In diesem Dokument wird folgendes Szenario behandelt: Wenn die Außenstelle über eine DIA-Verbindung (Direct Internet Access) verfügt, können Sie die Leistung verbessern, indem Sie den SaaS-Datenverkehr unter Umgehung des Rechenzentrums über die lokale DIA weiterleiten.



Hinweis: Die Konfiguration von Cloud OnRamp für SaaS, wenn ein Standort ein Loopback als TLOC-Schnittstelle (Transport Locator) verwendet, wird nicht unterstützt.

Konfigurieren

Netzwerkdiagramm

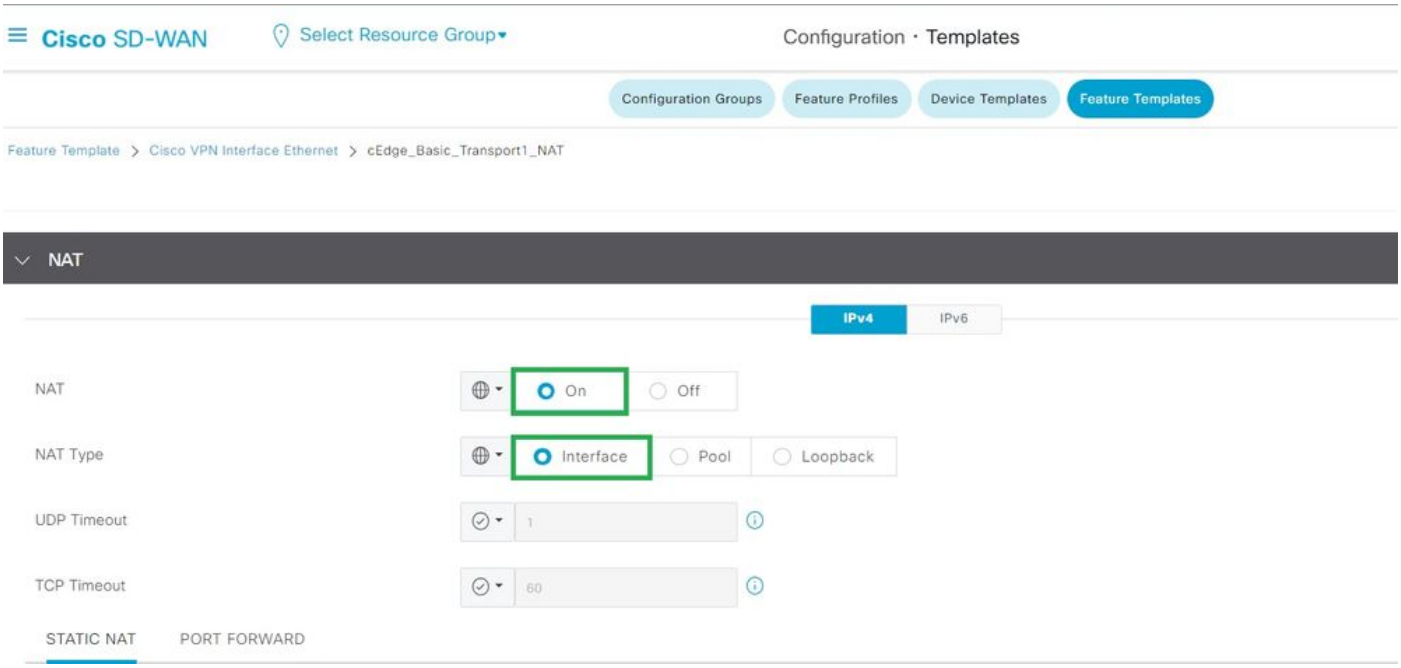


Netzwerktopologie

Konfigurationen

NAT auf der Transportschnittstelle aktivieren

Navigieren Sie zu Feature Template . Wählen Sie die **Transport VPN interface** Vorlage aus, und **aktivieren Sie NAT**.



NAT für Schnittstelle aktivieren

CLI-äquivalente Konfiguration:

```
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
```

Erstellen einer zentralisierten AAR-Richtlinie

Um eine zentrale Richtlinie einzurichten, müssen Sie dieses Verfahren befolgen:

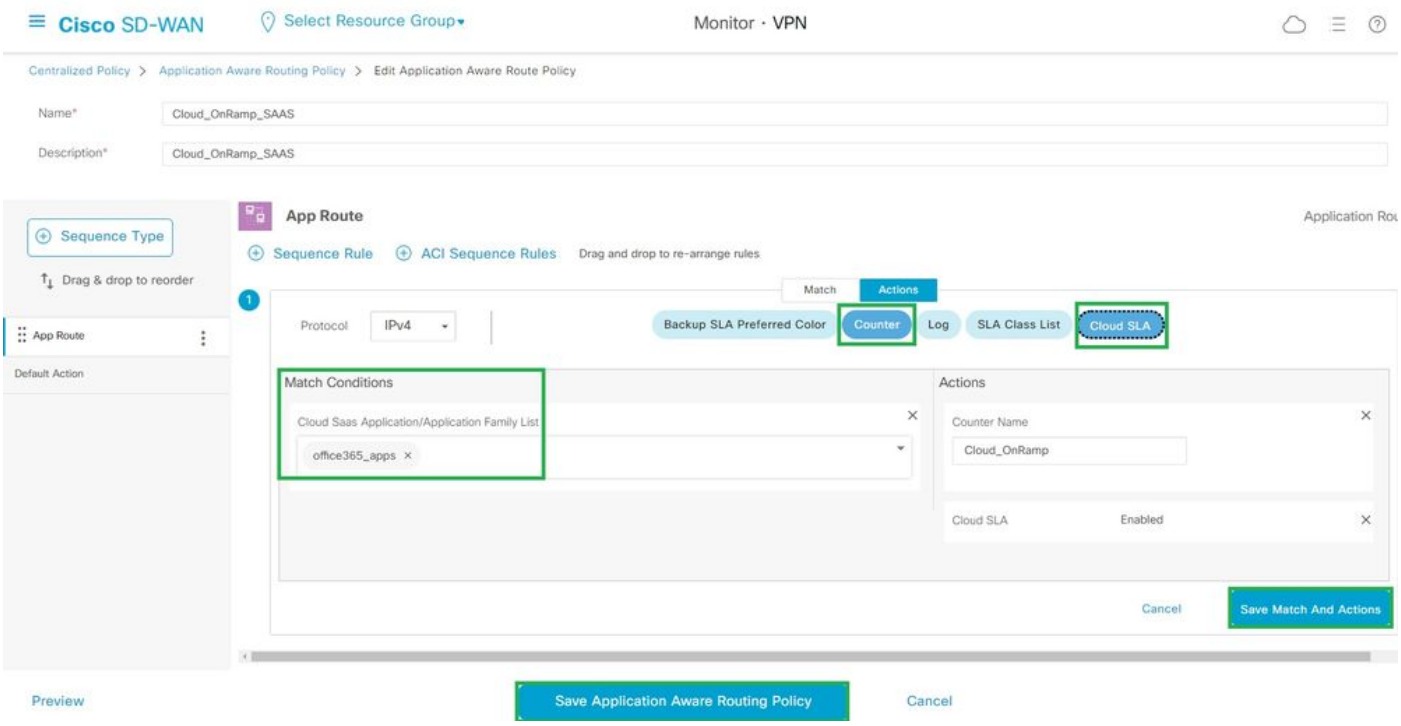
Schritt 1: Erstellen einer Standortliste:

NAT-Vorlage für VPN-Schnittstelle

Schritt 2: VPN-Liste erstellen:

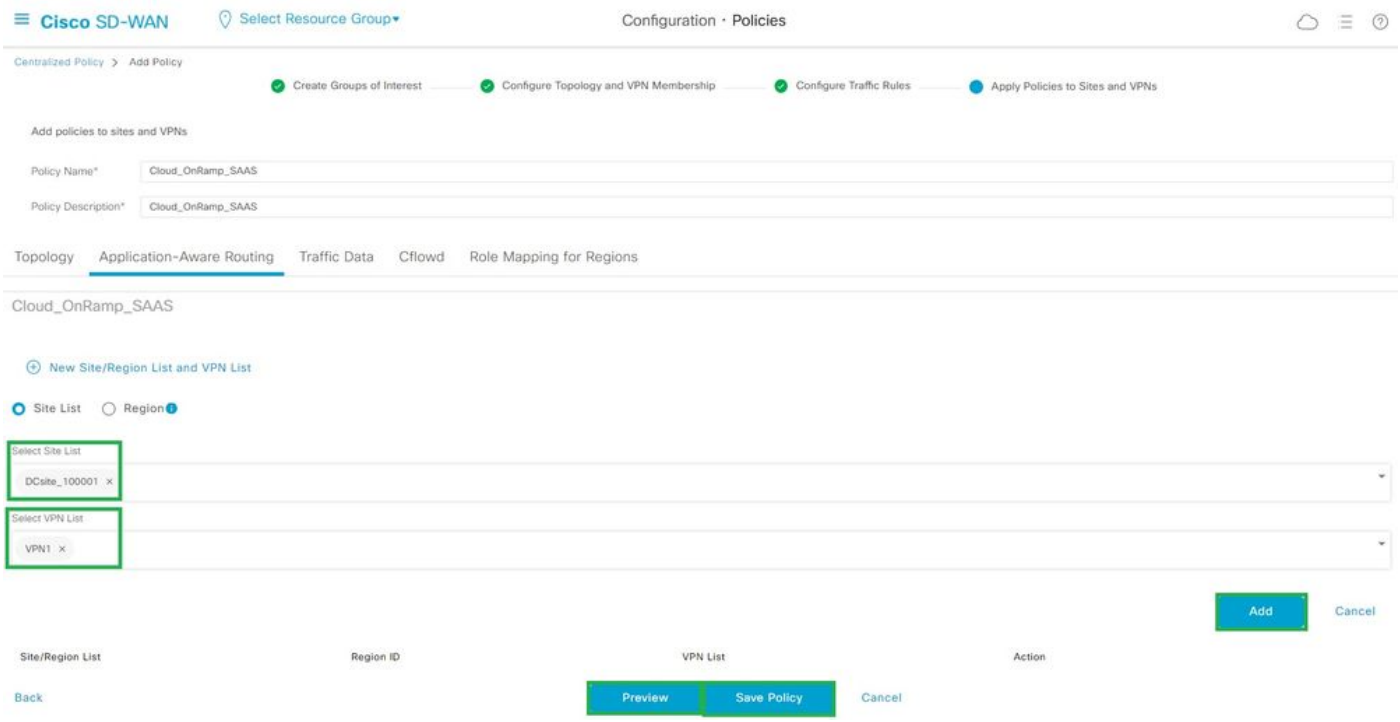
Benutzerdefinierte Siteliste für zentrale Richtlinie

Schritt 3: Konfigurieren Sie die Traffic Rules und erstellen Sie die Application Aware Routing Policy.



Anwendungssensitive Routing-Richtlinie

Schritt 4: Fügen Sie die Richtlinie dem vorgesehenenSites hinzu, und VPN:



Hinzufügen von Richtlinien zu Standorten und VPNs

CLI-äquivalente Richtlinie:

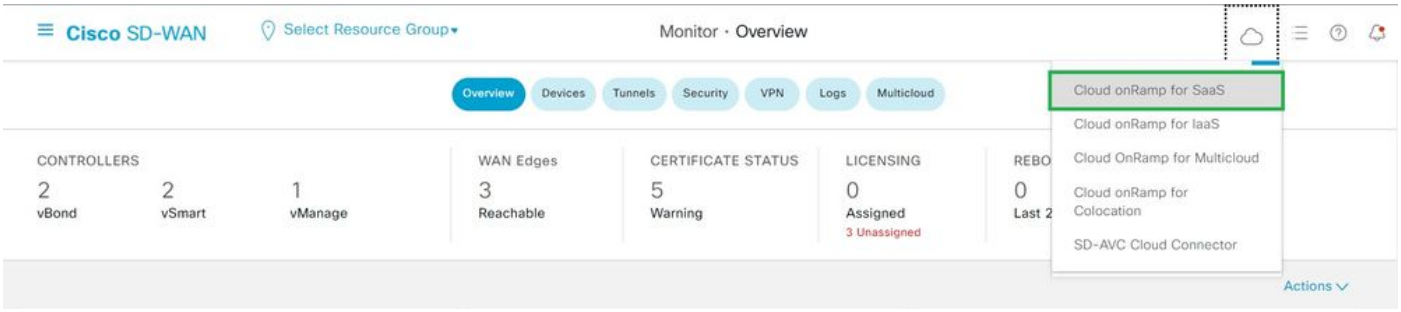
viptela-policy:policy
app-route-policy _VPN1_Cloud_OnRamp_SAAS
vpn-list VPN1
sequence 1

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
!
!
```

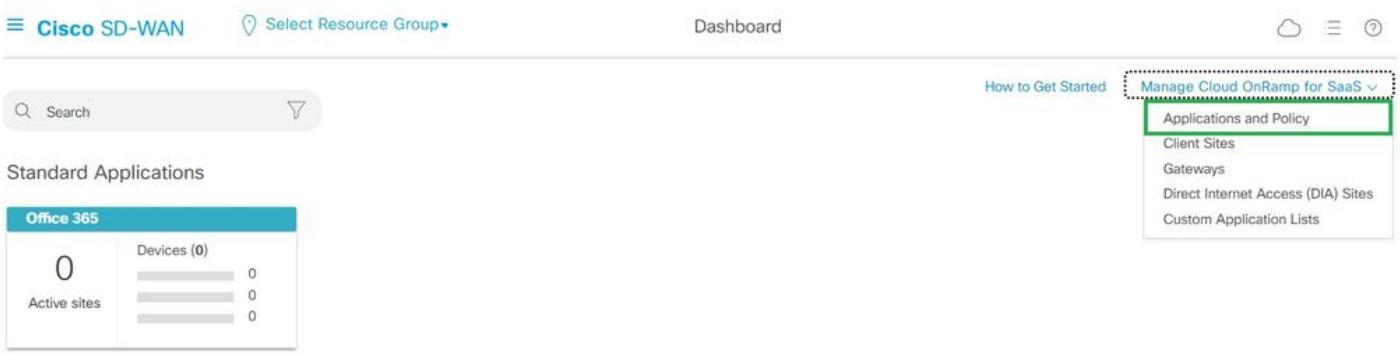
Aktivieren von Anwendungs- und direktem Internetzugriff in vManage

Schritt 1: Navigieren Sie zu Cloud OnRamp for SaaS.



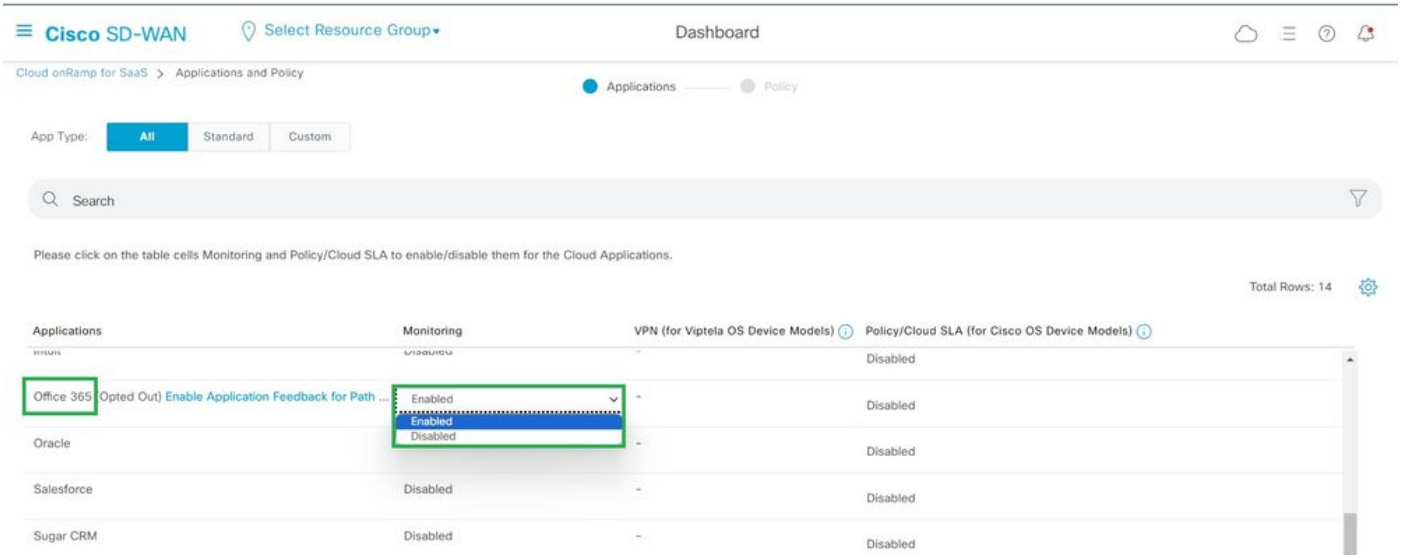
Wählen Sie Cloud onRamp für SaaS

Schritt 2: Navigieren Sie zu Applications and Policy.



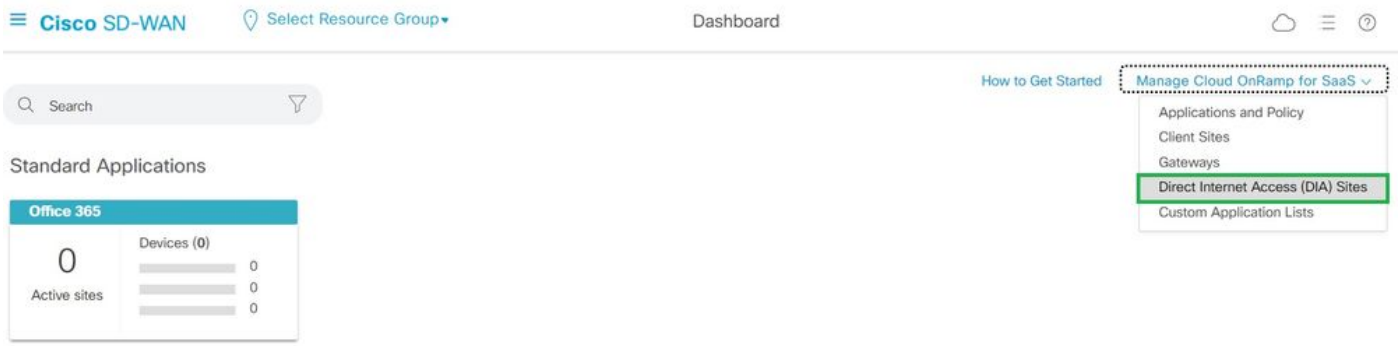
Auswählen von Anwendungen und Richtlinien

Schritt 3: Navigieren Sie zu Application > Enableund Save. Klicken Sie dann auf Next.



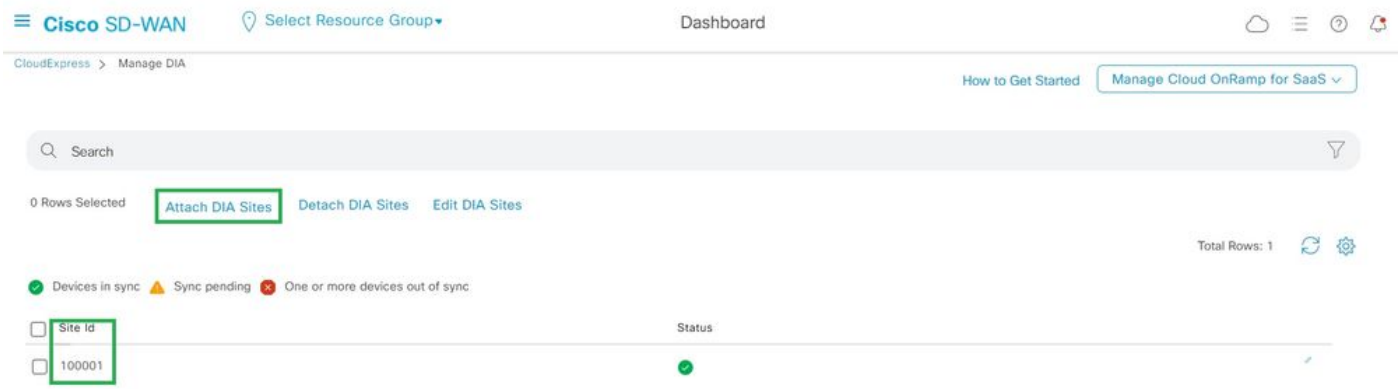
Anwendungen auswählen und Überwachung aktivieren

Schritt 4: Navigieren Sie zu Direct Internet Access (DIA) Sites.



Direkten Internetzugriff auswählen

Schritt 5: Navigieren Sie zu, Attach DIA Sites und wählen Sie Sites aus.



DIA-Standorte anhängen

Verifizierung

In diesem Abschnitt werden die Ergebnisse zur Verifizierung der Cloud-OnRamp für SaaS beschrieben.

- Diese Ausgabe zeigt CloudExpress local-exits:

```
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
```

- Diese Ausgabe zeigt CloudExpress-Anwendungen:

```
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
```

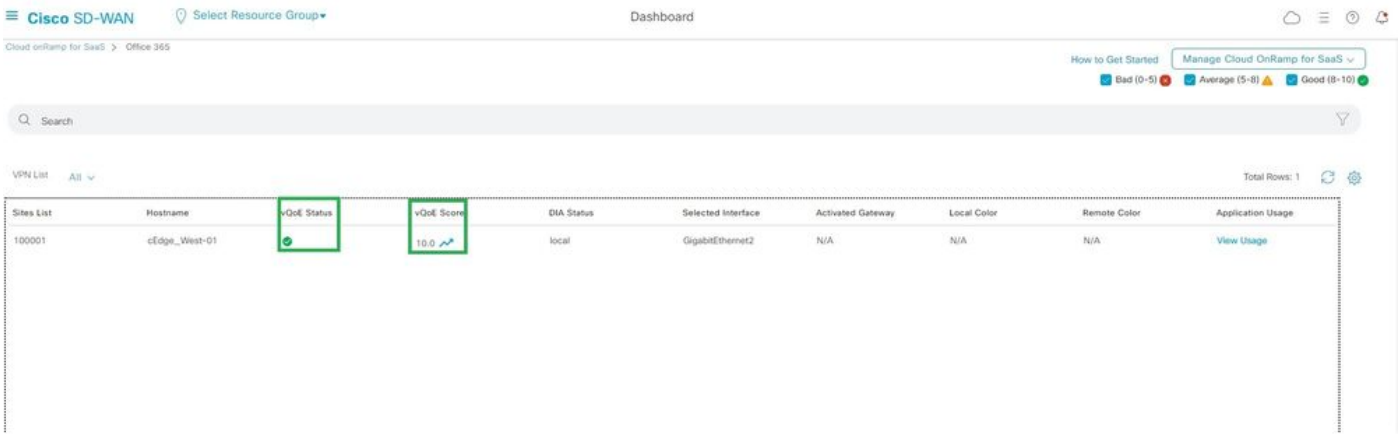
- Diese Ausgabe zeigt Zähler für interessierten Datenverkehr inkrementiert an:

<#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
```

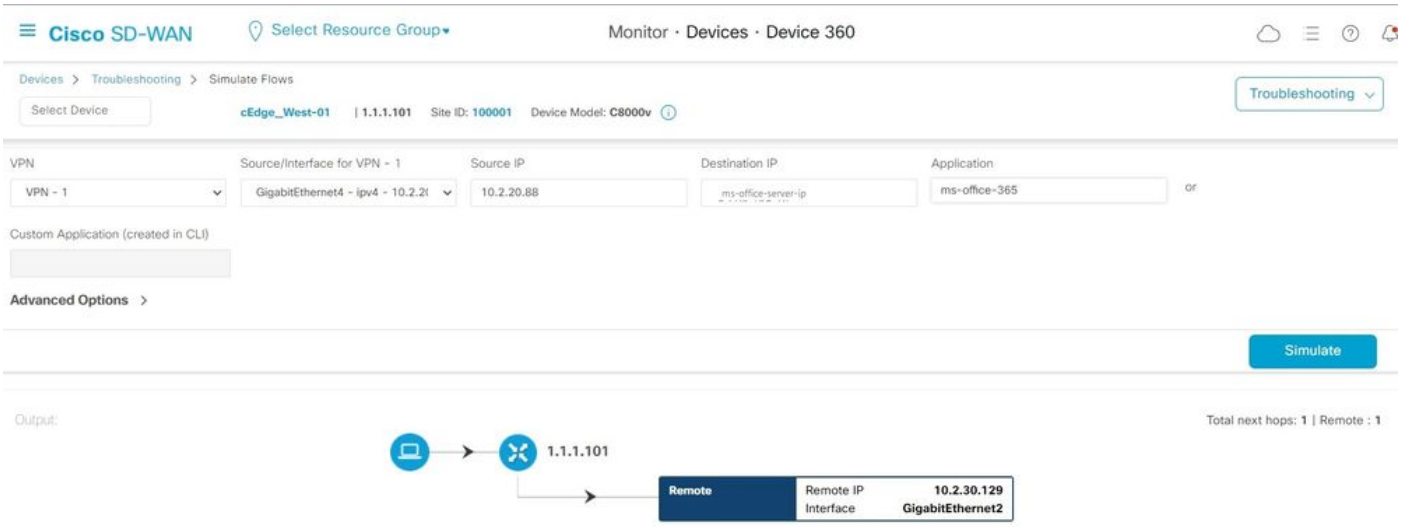
Cloud_OnRamp_-403085179 600 432292

- Diese Ausgabe zeigt den vQoE-Status und die Bewertung an:



vQoE-Status und -Bewertung

- Diese Ausgabe zeigt den Dienstpfad der vManage-GUI:



Servicepfad

- Diese Ausgabe zeigt den Dienstpfad von der Geräte-CLI an:

```
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
```

Zugehörige Informationen

- Cisco Catalyst SD-WAN Cloud OnRamp - Konfigurationsleitfaden
- Technischer Support und Downloads von Cisco

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.