Configurazione di SD-WAN Cloud onRamp per SaaS

Sommario

- Introduzione
- Prerequisiti
  - Requisiti
  - Componenti usati
- Premesse
- Configurazione
  - Esempio di rete
  - Configurazioni
    - Abilita NAT sull'interfaccia di trasporto
    - Creazione di un criterio AAR centralizzato
    - Abilitare l'accesso diretto a Internet e all'applicazione in vManage
- Verifica
- Informazioni correlate

Introduzione

Questo documento descrive la configurazione per Cloud onRamp for Software as a Service (SaaS) con uscita locale da filiale.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di Cisco Software-Defined Wide Area Network (SD-WAN).

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

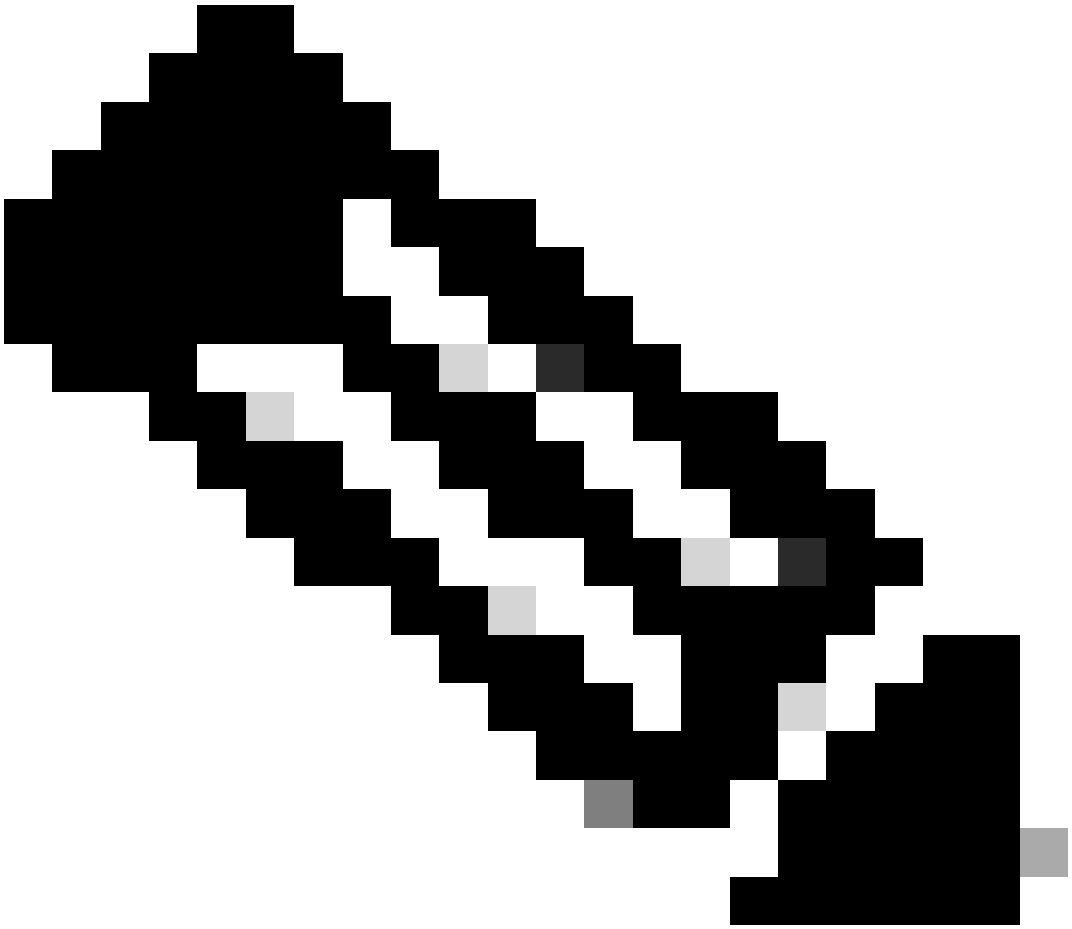
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Per un'organizzazione che utilizza SD-WAN, un sito di succursale in genere instrada il traffico delle applicazioni SaaS per impostazione predefinita su collegamenti di overlay SD-WAN verso un centro dati. Dal centro dati, il traffico SaaS raggiunge il server SaaS.

Ad esempio, in un'organizzazione di grandi dimensioni con un centro dati centrale e sedi distaccate, i dipendenti possono utilizzare Office 365 presso una sede distaccata. Per impostazione predefinita, il traffico di Office 365 in un sito di succursale viene instradato tramite un collegamento di overlay SD-WAN a un centro dati centralizzato e, dall'uscita DIA, al server cloud di Office 365.

Questo documento descrive questo scenario: se il sito di succursale dispone di una connessione DIA (Direct Internet Access), è possibile migliorare le prestazioni instradando il traffico SaaS attraverso la connessione DIA locale, ignorando il centro dati.



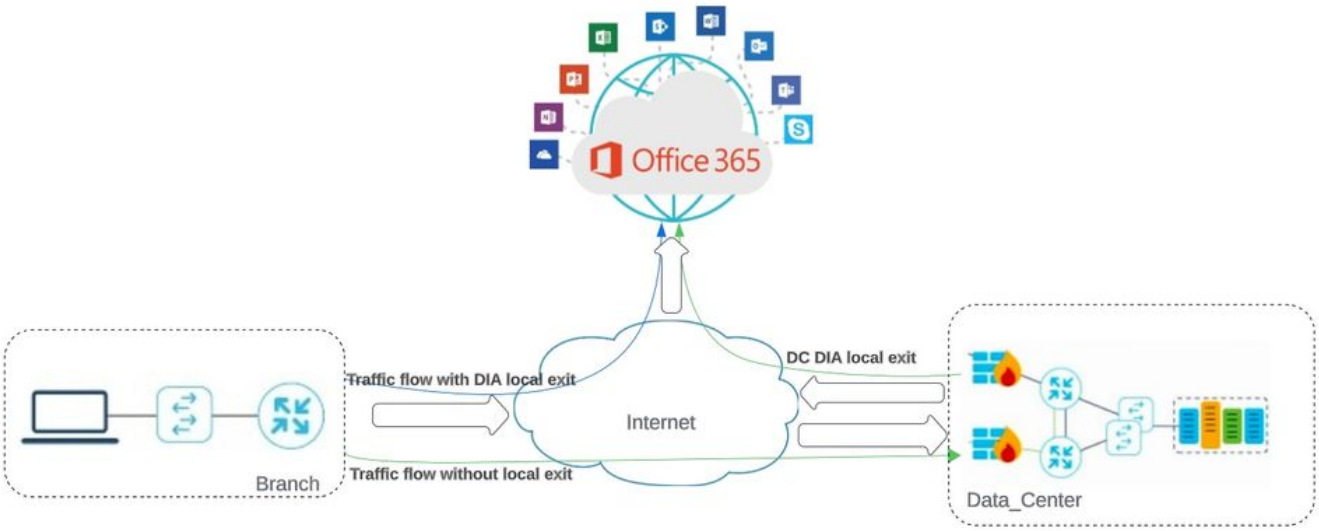
Nota: la configurazione di Cloud onRamp per SaaS quando un sito utilizza un loopback

---

come interfaccia TLOC (Transport Locator) non è supportata.

Configurazione

Esempio di rete

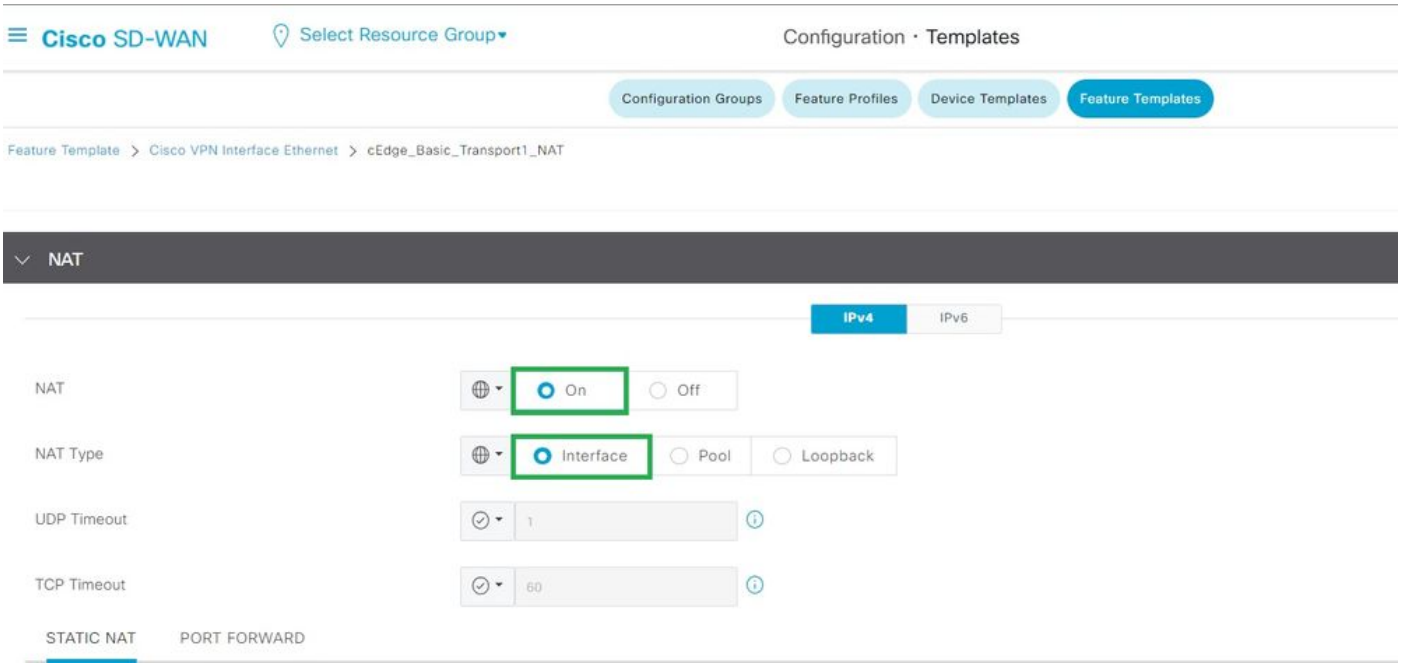


Topologia della rete

Configurazioni

Abilita NAT sull'interfaccia di trasporto

Passare a Feature Template . Scegliere il **Transport VPN interface** modello e **abilitare NAT**.



Abilita interfaccia NAT

Configurazione equivalente 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

Creazione di un criterio AAR centralizzato

Per stabilire una policy centralizzata, devi attenerti a questa procedura:

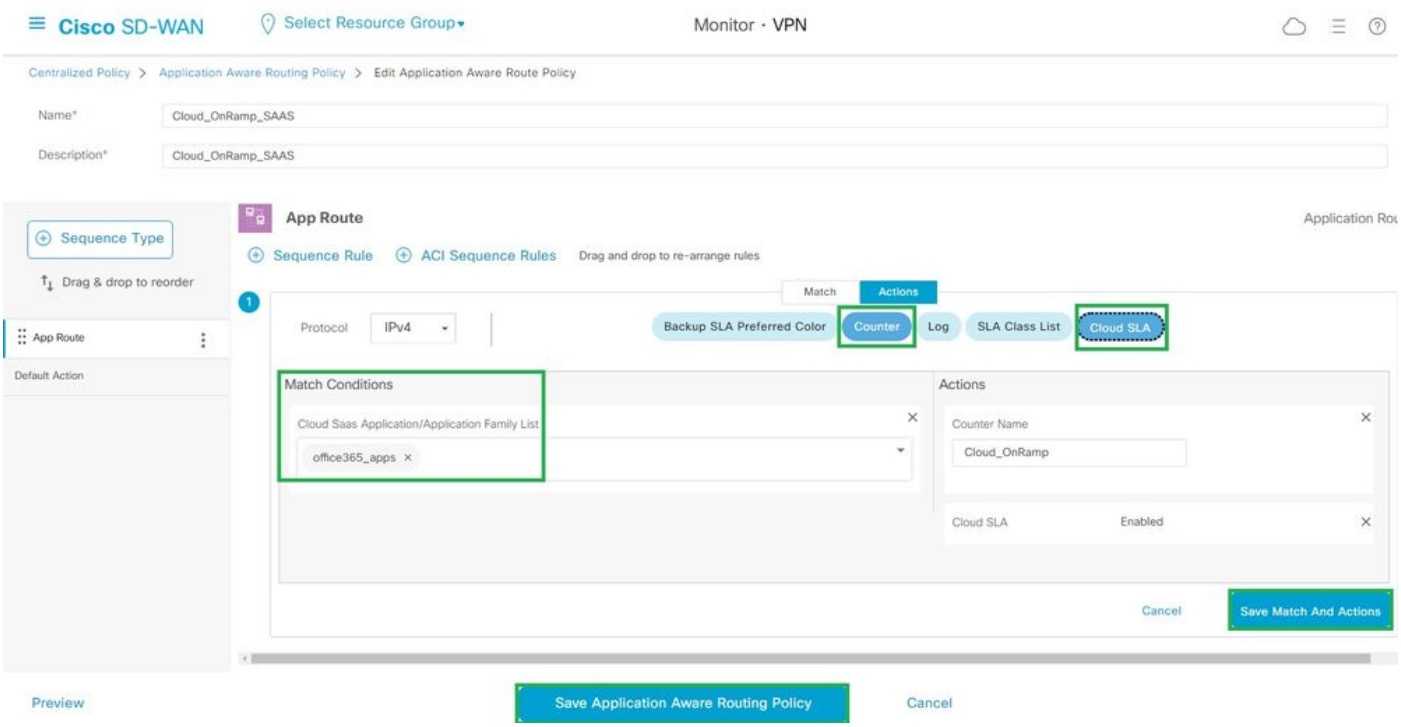
Passaggio 1. Creare un elenco Sito:

Modello VPN Interface NAT

Passaggio 2. Creare un elenco VPN:

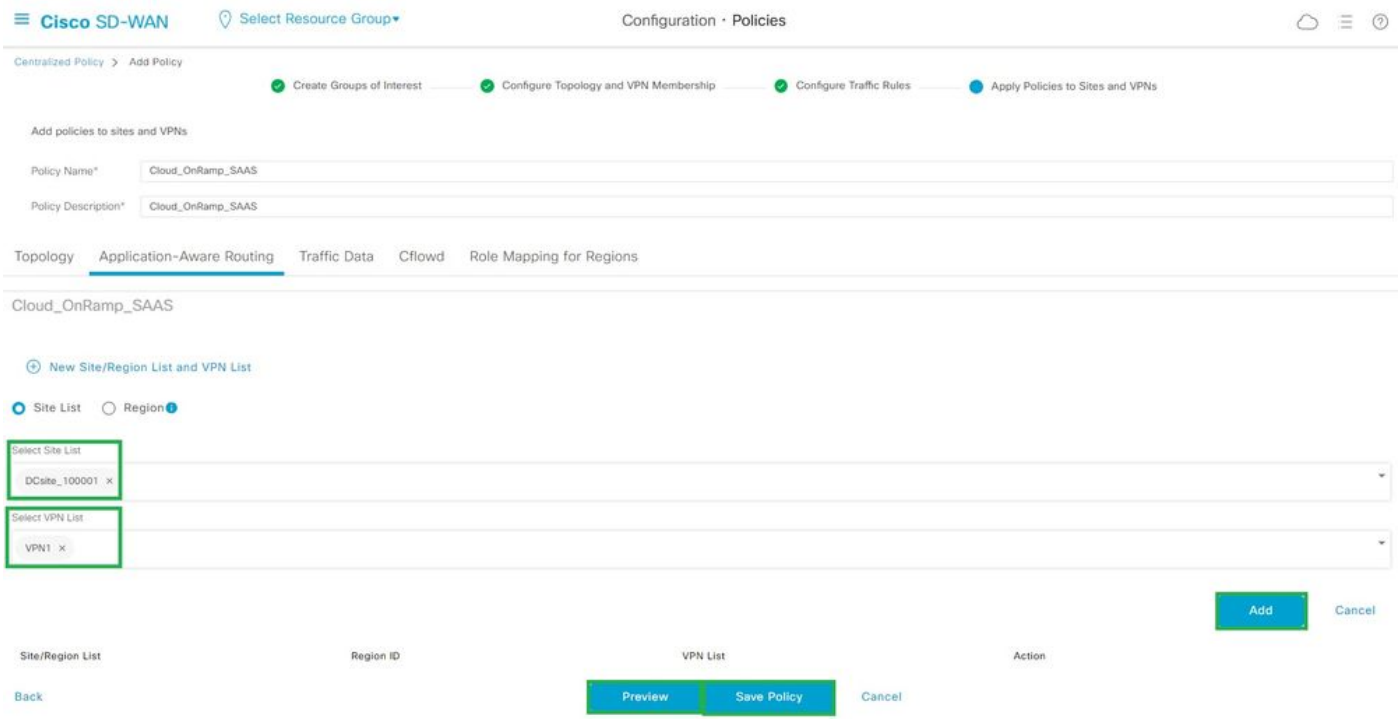
Elenco siti personalizzato criteri centralizzati

Passaggio 3. Configurare il Traffic Rules e creare il Application Aware Routing Policy.



Criterio route con riconoscimento dell'applicazione

Passaggio 4. Aggiungere il criterio alla destinazioneSites e VPN:



Aggiungi criteri a siti e VPN

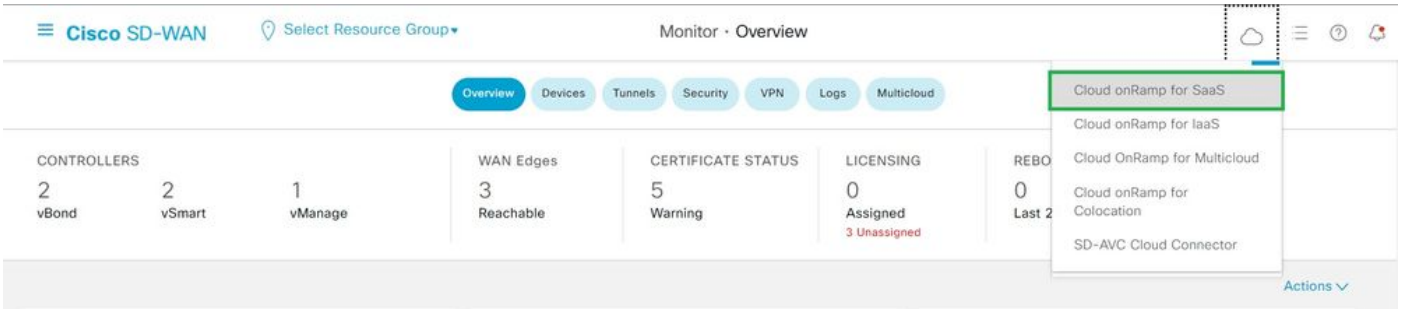
Criteri equivalenti CLI:

```
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
!
!
```

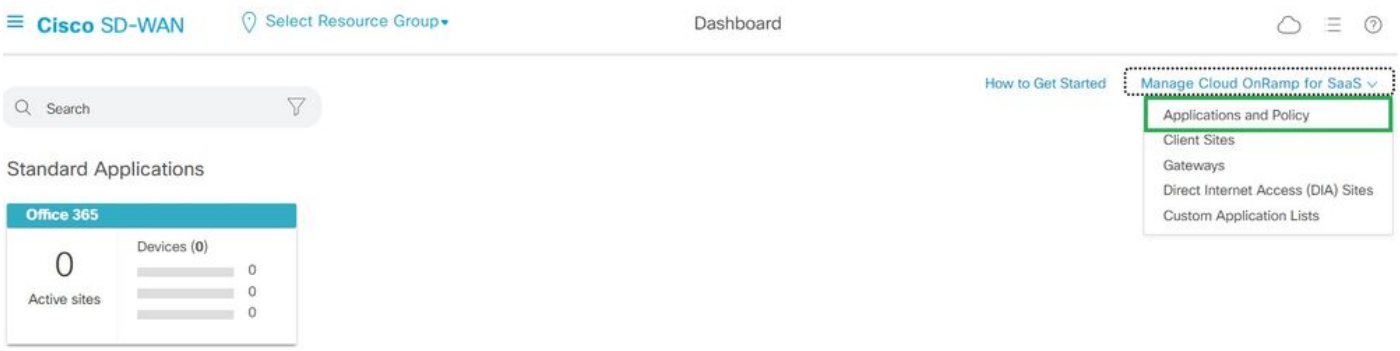
Abilitare l'accesso diretto a Internet e all'applicazione in vManage

Passaggio 1. Passare a Cloud OnRamp for SaaS.



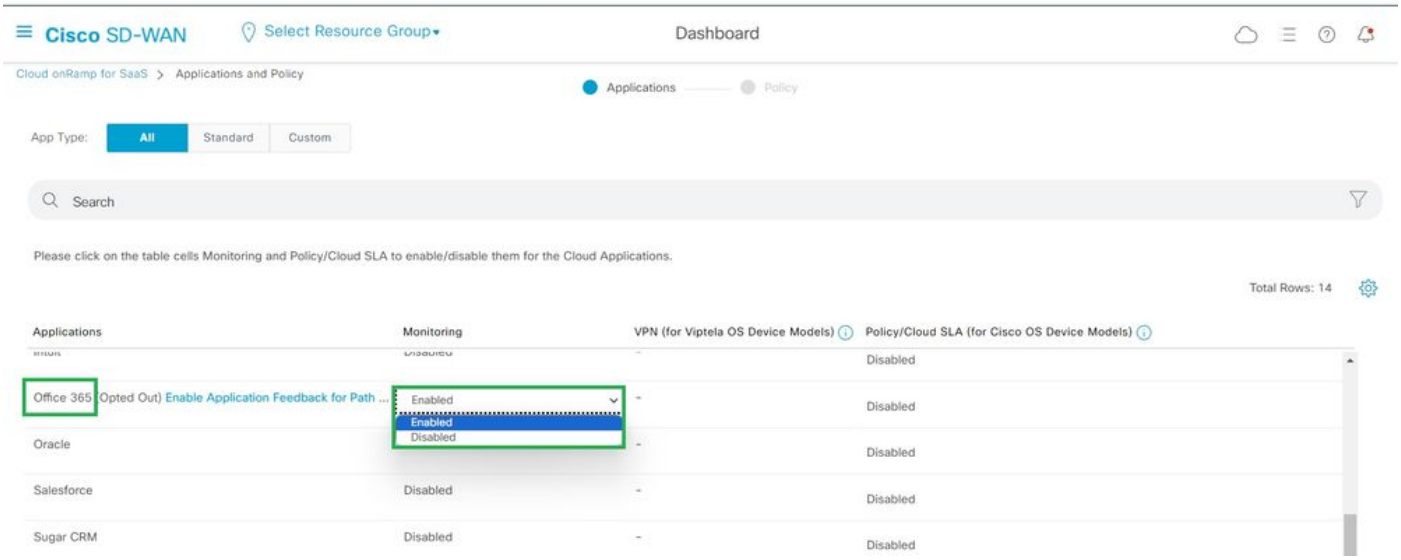
Seleziona Cloud onRamp per SaaS

Passaggio 2. Passare a Applications and Policy.



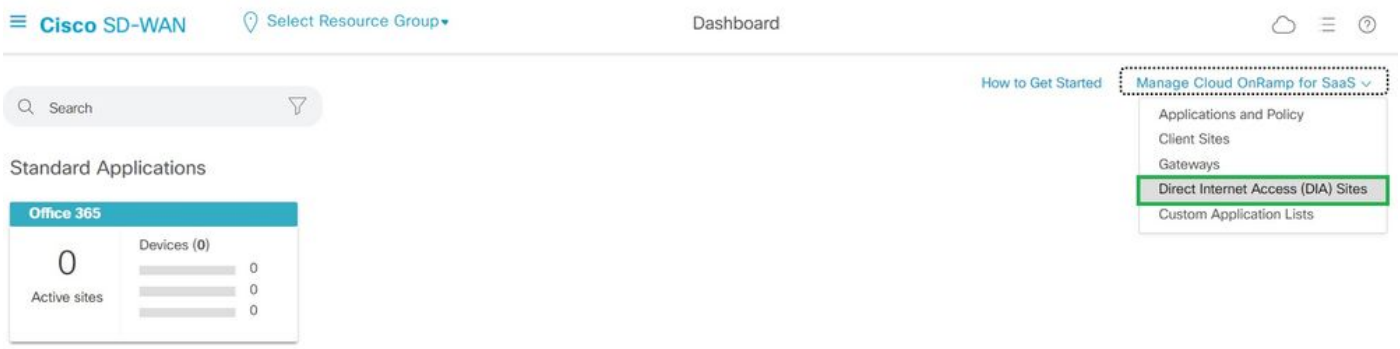
Seleziona applicazioni e criteri

Passaggio 3. Passare a Application > Enablee Save. Quindi fate clic su Next.



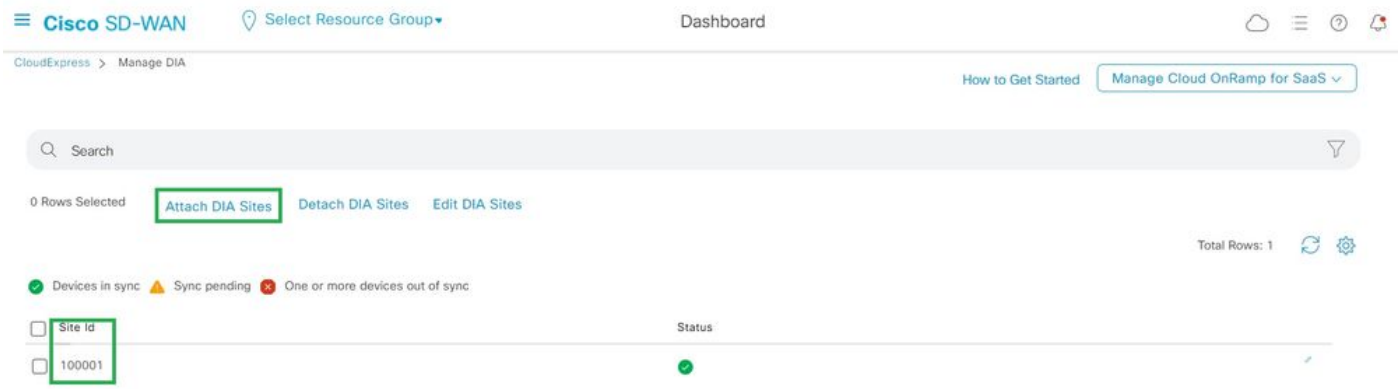
Seleziona applicazioni e abilita monitoraggio

Passaggio 4. Passare a Direct Internet Access (DIA) Sites.



Seleziona siti con accesso diretto a Internet

Passaggio 5. Individuare Attach DIA Sites e scegliere i siti.



Collega siti DIA

Verifica

In questa sezione vengono descritti i risultati per verificare Cloud onRamp per SaaS.

- Questo output mostra le uscite locali di 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
```

- Questo output mostra le applicazioni 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
```

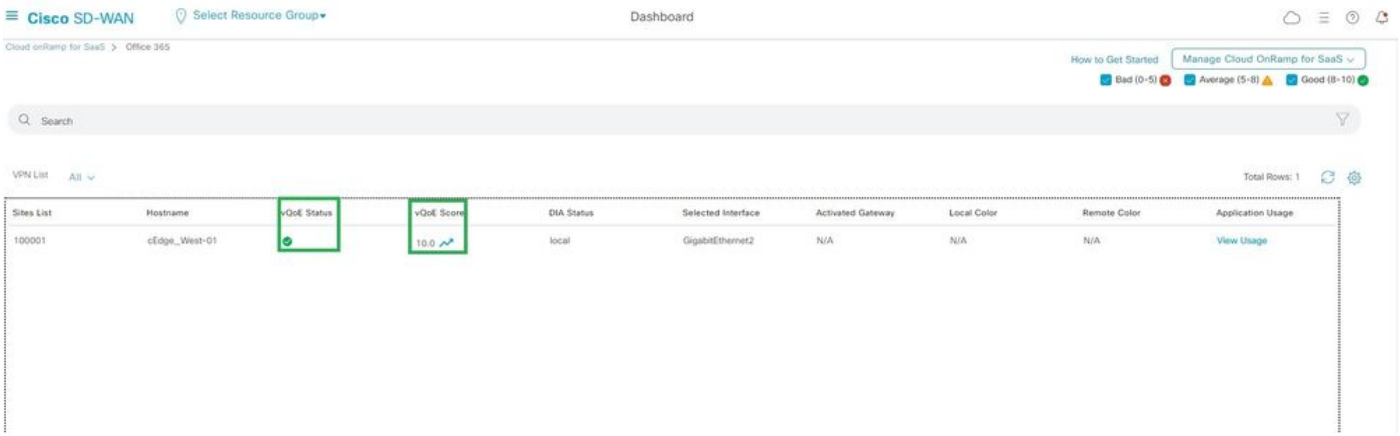
- In questo output vengono mostrati i contatori incrementali per il traffico interessato:

<#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
```

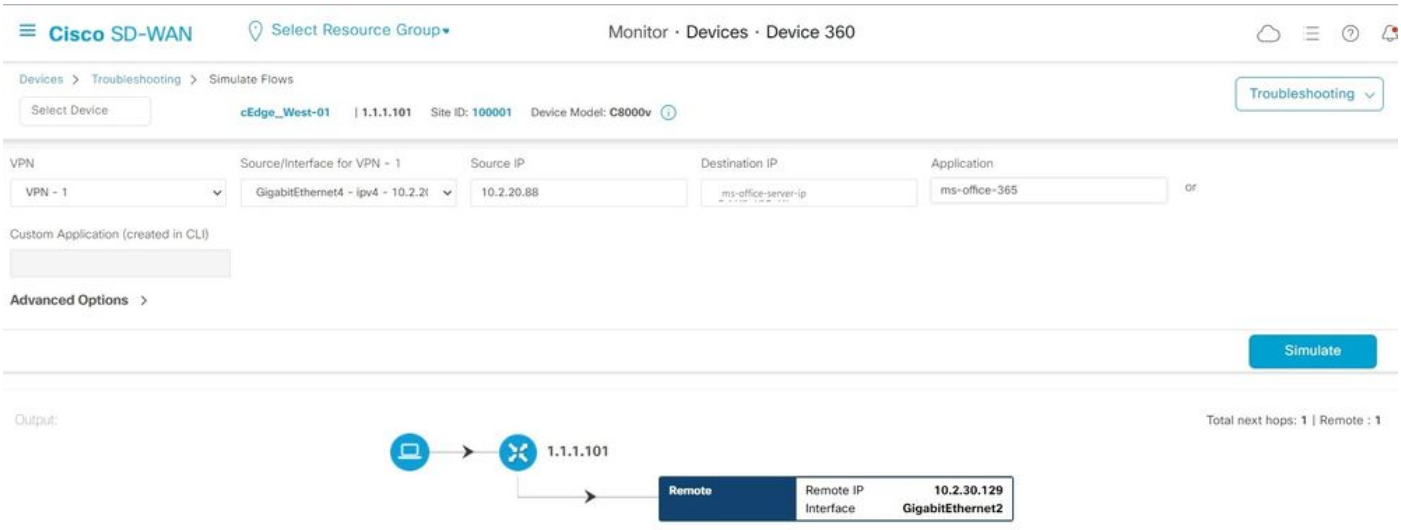
Cloud_OnRamp_-403085179 600 432292

- Questo output mostra lo stato e il punteggio vQoE:



Stato e punteggio vQoE

- Questo output mostra il percorso del servizio dalla GUI vManage:



Percorso servizio

- Questo output mostra il percorso del servizio dalla 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
```

Informazioni correlate

- Guida alla configurazione di Cisco Catalyst SD-WAN Cloud onRamp
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).