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

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.

Cisco SD-WAN	Select Resource Group•		Configuration ·	Templates
		Configuration Groups	Feature Profiles	Device Templates Feature Templates
iture Template > Cisco VPN Int	erface Ethernet > cEdge_Basic_Transport1_NAT			
NAT				
			IPv4	IPv6
NAT	⊕ • ○ On	O Off		
NAT Type	• • O Inter	face O Pool	🔿 Loopback	
UDP Timeout	Ø • 1	0		
TCP Timeout	Ø • 60	0		
STATIC NAT PORT FO	DRWARD			

Abilita	inte	rfac	cia	NAT
11011111	inic	ijuc	сш	TATT

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:

≡ (Cisco SD-WAN	O Select Resource O	Broup -	Configuration · P	olicies		
Centra	lized Policy > Define Lists						ှိုး c
Select	a list type on the left and start	creating your groups of interes	st				
Applic Color	ation	New Site List					
Comm	unity	Name	Entries	Reference Count	Updated By	Last Updated	Action
Police	r	DCsite_100001	100001	3	admin	11 Sep 2023 12:46:54 PM P	000
Prefix							

Passaggio 2. Creare un elenco VPN:

≡ Cisco SD-WAN	Select Resource	e Group •	Configuration ·	Policies		
Centralized Policy > Define Lists						ိုး၊ c
Select a list type on the left and star	rt creating your groups of inte	rrest				
Application	O New City List	_				
Color	(+) New Site List					
Community						
Data Prefix	Name	Entries	Reference Count	Updated By	Last Updated	Action
Policer	DCsite_100001	100001	3	admin	11 Sep 2023 12:46:54 PM P	100
Prefix						
Site						

Elenco siti personalizzato criteri centralizzati

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

Application	Aware R	outing Policy > Edit Application Aware Route Policy				
Cloud_On	Ramp_SA	AS				
Cloud_Or	Ramp_SA	VAS				
pe reorder	• •	App Route Sequence Rule ACI Sequence Rules Drag and drop to re-arrange rules Match Actic Protocol IPv4 Backup SLA Preferred Color Counter	Lc	og SLA Class List	Cloud SLA	Application f
		Match Conditions	~	Actions		~
		Cloud Saas Application/Application Family List office365_apps ×	Î	Counter Name Cloud_OnRamp		~
				Cloud SLA	Enabled	×
					Cancel	, Save Match And Actions
	Application Cloud_Or Cloud_Or reorder :	Application Aware R Cloud_OnRamp_S/ Cloud_OnRamp_S/ Pe reorder	Application Aware Routing Policy > Edit Application Aware Route Policy Cloud_OnRamp_SAAS Cloud_OnRamp_SAAS Cloud_OnRamp_SAAS Performed Policy Protocol IPv4 Backup SLA Preferred Color Counter Match Conditions Cloud Sass Application/Application Family List office365_apps ×	Application Aware Routing Policy > Edit Application Aware Route Policy Cloud_OnRamp_SAAS Cloud_OnRamp_SAAS Cloud_OnRamp_SAAS Pereorder Protocol IPv4 Reackup SLA Preferred Color Counter Le Match Cloud Saas Application/Application Family List office365_apps ×	Application Aware Routing Policy > Edit Application Aware Route Policy Cloud_OnRamp_SAAS Cloud_OnRamp_SAAS Cloud_OnRamp_SAAS Per Protocol IPv4 Backup SLA Preferred Color Counter to g SLA Class List Match Conditions Cloud SLA Cloud SLA Cloud SLA	Application Aware Routing Policy > Edit Application Aware Route Policy Cloud_OnRamp_SAAS Cloud_OnRamp_SAAS Cloud_OnRamp_SAAS Performer Over Cloud Over Clo

Criterio route con riconoscimento dell'applicazione

Passaggio 4. Aggiungere il criterio alla destinazioneSites e VPN:

E Cisco SD-WAN	esource Group+	Configuration · Po	olicies		
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 Rol	le Mapping for Regions			
Cloud_OnRamp_SAAS					
New Site/Region List and VPN List					
Site List O Region					
Select Site List					
DCsite_100001 ×					Ŷ
Select VPN List					
VPN1 ×					*
					Add Cancel
Site/Region List	Region ID	VPN List		Action	
Back		Preview S	ave Policy Cancel		
Aggiungi criteri a siti e VPN					
Criteri equivalenti CLI:					
viptela-policy:policy app-route-policy _VPN1_Clou vpn-list VPN1 sequence 1 match cloud-saas-app-list office365_: source-ip 0.0.0.0/0 !	ıd_OnRamp_SAAS apps				
action count Cloud OnRamp -92622	2761				
!					
!					
!					
ists					
app-list office365_apps					
ipp skype					
app ms_communicator					
app livemail mobile					
pp word_online					
app excel_online					
app onedrive					
app yammer					
app sharepoint					
app ms-office-365					
app nockeyapp					
app live_notman					
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.

= Cisco	SD-WAN	V Select Resource Group+		Monitor · Overview			0	≡ ⊘
			Overview Devices	Tunnels Security VPN	Logs Multicloud	1	Cloud onRamp for SaaS	1
ONTROLLER	RS		WAN Edges	CERTIFICATE STATUS	LICENSING	REBO	Cloud onRamp for laaS Cloud OnRamp for Multicloud	-
2 Bond	2 vSmart	1 vManage	3 Reachable	5 Warning	O Assigned 3 Unassigned	() Last 2	Cloud onRamp for Colocation SD-AVC Cloud Connector	

Seleziona Cloud onRamp per SaaS

Passaggio 2. Passare a Applications and Policy.

≡ Cisco SD-V	NAN 📀 Select Resource Group -	Dashboard	$\bigcirc \equiv \odot$
Q Search	A .	How to Get Starte	d Manage Cloud OnRamp for SaaS v
Standard Applic	cations		Client Sites Gateways Direct Internet Access (DIA) Sites Custom Application Lists
O Active sites	Devices (0) 0 0 0		

Seleziona applicazioni e criteri

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

≡ Cisco SD-WAN ③ Select	Resource Group+	Dashboa	ard	$\bigcirc \equiv \odot \bigcirc$
Cloud onRamp for SaaS > Applications and Policy		Applications	Policy	
App Type: All Standard Cust	om			
Q Search				∇
Please click on the table cells Monitoring and Poli	cy/Cloud SLA to enable/disable them for	the Cloud Applications.	S Davine Models)	Total Rows: 14 🔅
inture international internati	Lisauleu	-	Disabled	•
Office 365 Opted Out) Enable Application Feedba	ick for Path Enabled	· ·	Disabled	
Oracle	Disabled	-	Disabled	
Salesforce	Disabled	-	Disabled	
Sugar CRM	Disabled	1711	Disabled	

Seleziona applicazioni e abilita monitoraggio

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

≡ Cisco SD-V	NAN 🛇 Select Resource Group•	Dashboard	$\bigcirc \equiv \odot$
Q Search	\overline{Y}	How to Get Started	Manage Cloud OnRamp for SaaS v
Standard Applic	cations		Client Sites Gateways Direct Internet Access (DIA) Sites
Office 365			Custom Application Lists
O Active sites	0 0 0 0		

Seleziona siti con accesso diretto a Internet

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

E Cisco SD-WAN	⑦ Select Resource Group ▼	Dashboard			0 4
CloudExpress > Manage DIA			How to Get Started Manage	Cloud OnRamp for SaaS	~
Q Search				3	7
0 Rows Selected Attach	DIA Sites Detach DIA Sites Edit DIA Sites			Total Rows: 1 📿	@
🥑 Devices in sync 🛕 Sync pe	ending 😒 One or more devices out of sync				
Site Id		Status			
100001		۰		~	

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 pol-	icy app-route	e-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:

E Cisco SD-V	WAN 💮 Select Re	source Group+		0	lashboard				0	≡ ⊘	1 4
Cloud onRump for SauS	5 > Office 365							How to Get Started Bad (0-5) 👸	Manage Cloud OnRamp fo	or SaaS v)
Q Search										∇	
VPN List All 🗸									Total Rows: 1	0	2
Sites List	Hostname	vQoE Status	vQoE Score	DIA Status	Selected Interface	Activated Gateway	Local Color	Remote Color	Application Usage		
100001	cEdge_West-01	0	10.0 🞤	local	GigabitEthernet2	N/A	N/A	N/A	View Usage		
										1	

Stato e punteggio vQoE

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

= CISCO SD-WAN	Select Resource Group •	M	Ionitor · Devices · Device 360		$\bigcirc \equiv \odot l$		
Devices > Troubleshooting > Si	mulate Flows				Troubleshooting V		
Select Device	cEdge_West-01 1.1.1.101 Site ID	D: 100001 Device Model: C8	8000v 🕕				
/PN	Source/Interface for VPN - 1	Source IP	Destination IP	Application			
VPN - 1	GigabitEthernet4 - ipv4 - 10.2.2(🗸	10.2.20.88	ms-office-server-ip	ms+office+365	Or		
Advanced Options >							
Advanced Options >					Simulate		
Advanced Options >		> 😥 1.1.1.101			Simulate Total next hops: 1 Remote : 1		
Advanced Options >		> 🔀 1.1.1.101	Remote Remote IP Interface	10.2.30.129 GigabitEthernet2	Simulate Total next hops: 1 Remote : 1		

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
- <u>Supporto tecnico Cisco e download</u>

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).