

Configurare l'estensione TLOC utilizzando il modello di funzionalità vManage

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Esempio di rete](#)

[Configurazioni](#)

[Modello funzionalità VPN](#)

[Modello dispositivo](#)

[Verifica](#)

[Scenari d'uso](#)

[Limitazioni](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare l'estensione TLOC utilizzando il modello di funzionalità vManage.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Utilizzo del modello di funzionalità vManage
- Due (2) dispositivi vEdge devono essere caricati correttamente su vManage

Componenti usati

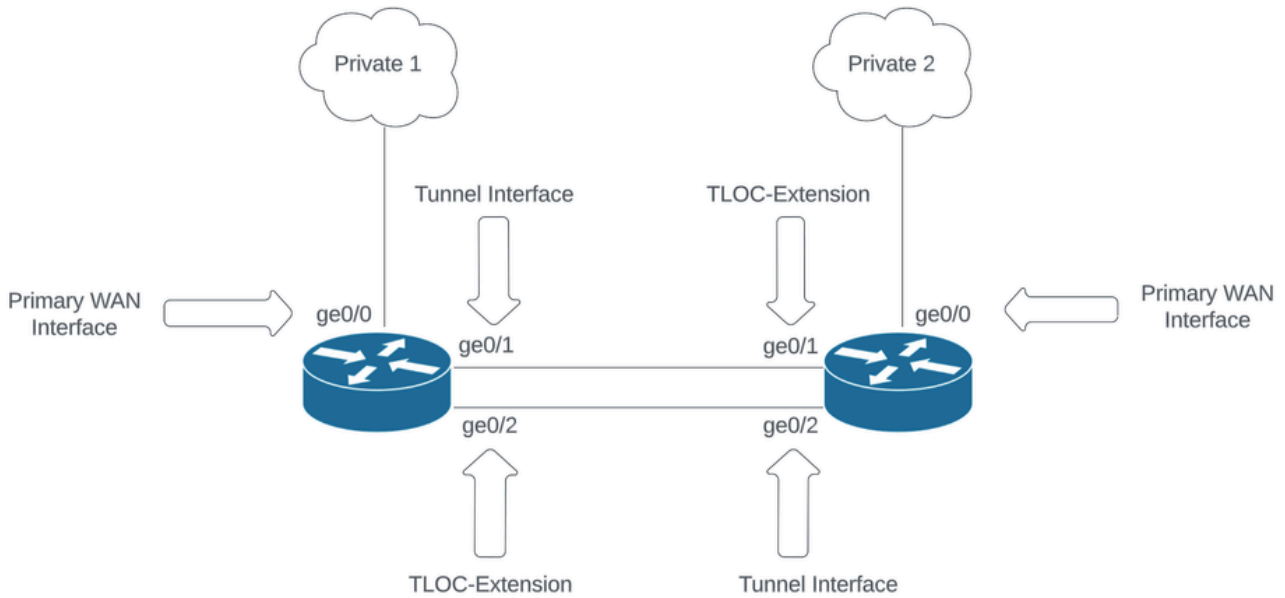
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco vManage versione 20.6.3
- vEdge 20.6.3

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.

Esempio di rete



Topologia della rete

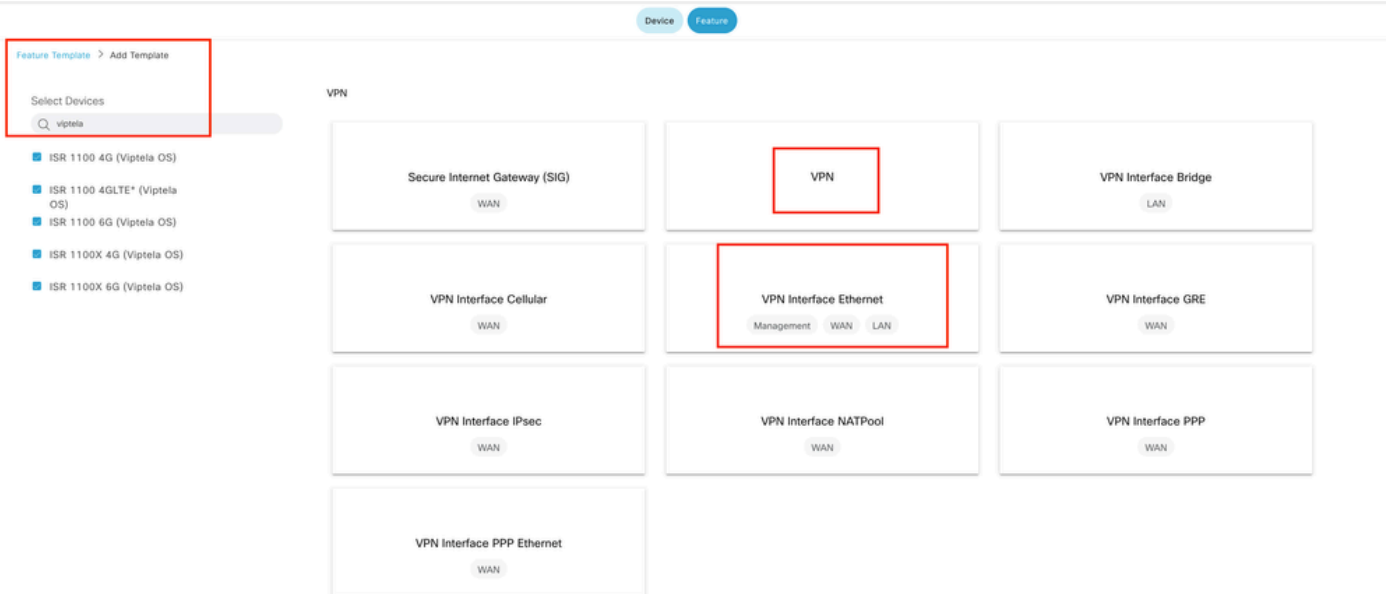
Configurazioni

In questo documento si presume che gli altri modelli di funzionalità siano già stati configurati. Lo stesso modello di workflow è applicabile ai dispositivi Cisco IOS® XE SD-WAN.

Creare un totale di 4 modelli di funzionalità da applicare al modello di dispositivo vEdge.

Modello funzionalità VPN

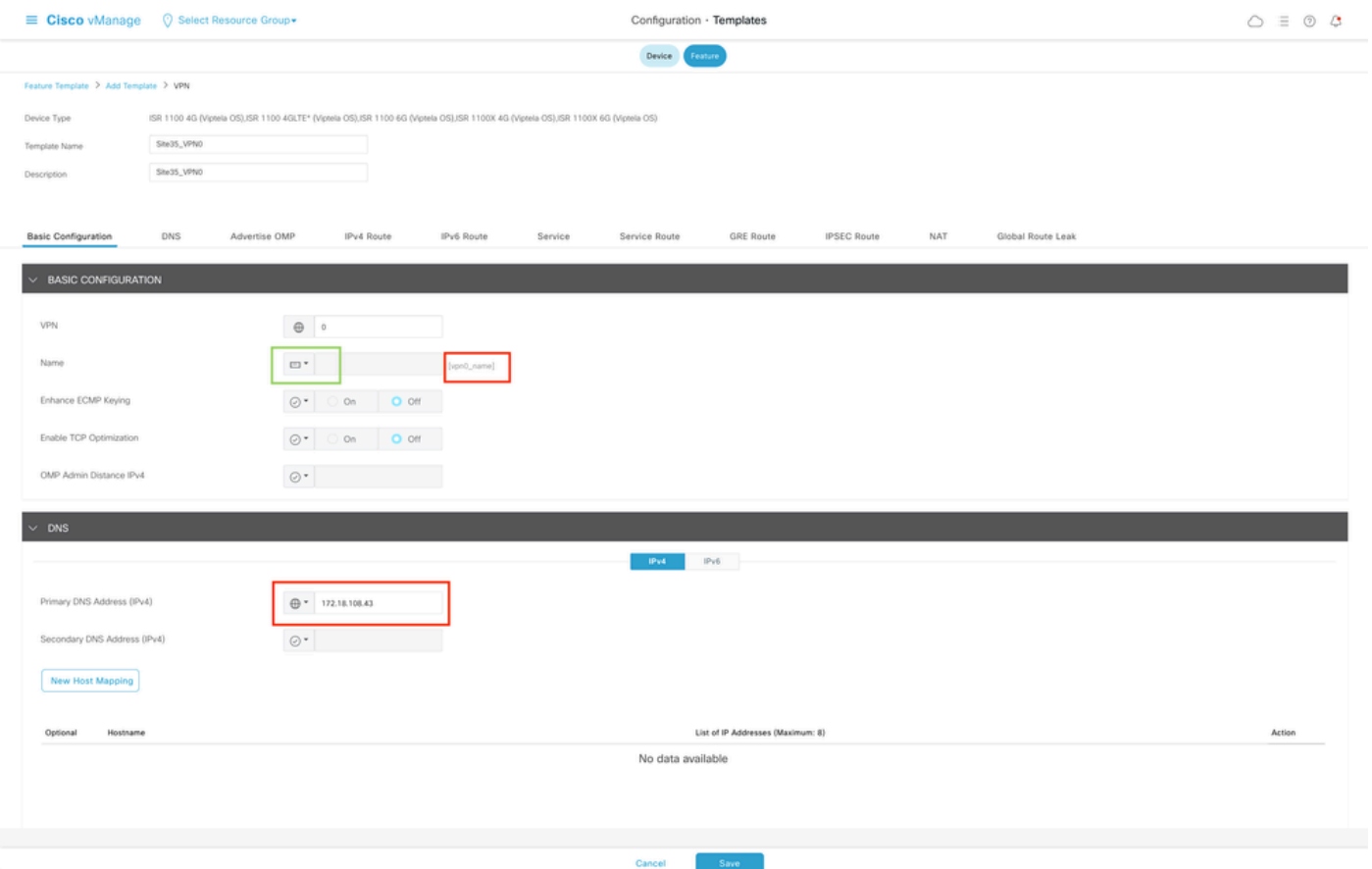
Questo modello di funzionalità include VPN 0, VPN Interface Ethernet (connessione WAN principale), VPN Interface Ethernet (Tunnel/NoTlocExt) e VPN Interface Ethernet (TlocExt/NoTunnel):



Modelli di funzionalità VPN

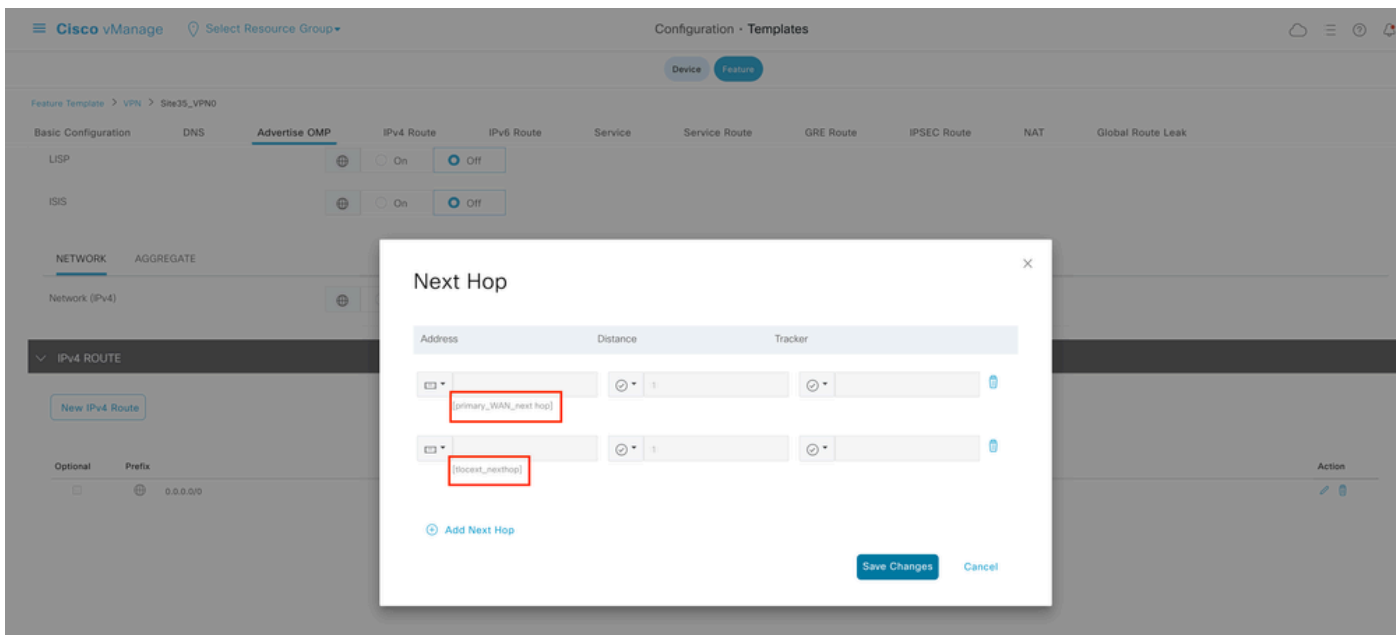
Passaggi per la creazione di modelli di feature:

1. VPN 0: selezionare il valore del dispositivo specifico per Transport VPN nella sezione di configurazione di base e aggiungere l'indirizzo del server DNS nella sezione DNS:

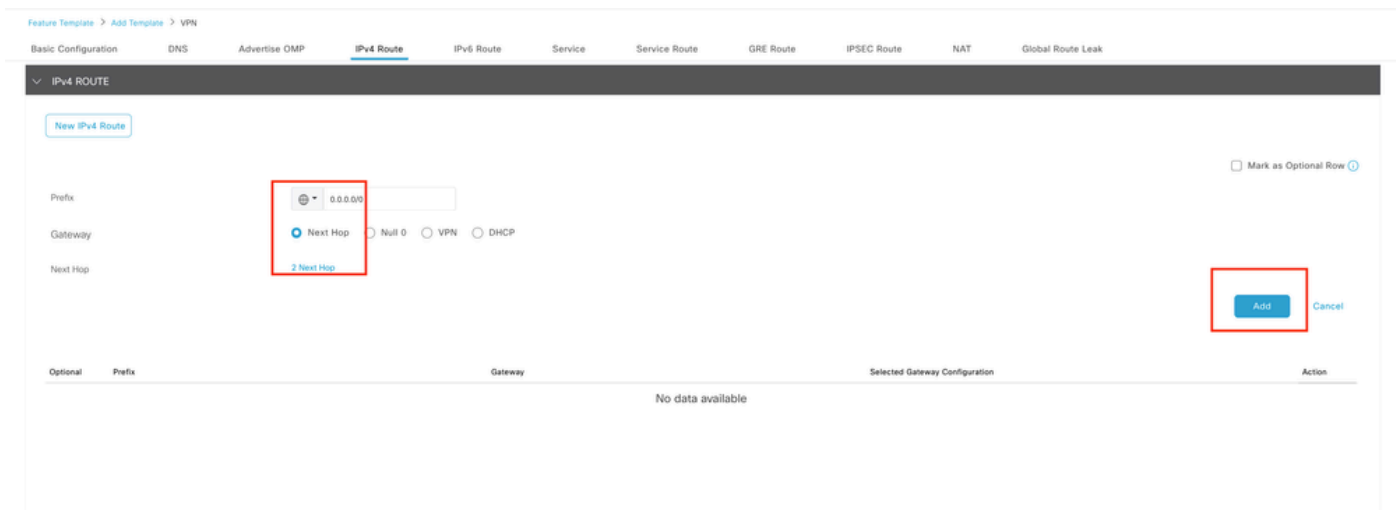


Configurazione base modello funzionalità VPN 0

Aggiungere un prefisso con valori specifici del dispositivo per l'indirizzo dell'hop successivo 2 (WAN primaria e TCP-EST) nella sezione della route IPv4:



Route IPv4 modello funzionalità VPN 0



Hop successivo route IPv4 modello funzionalità VPN 0

2. VPN Interface Ethernet (Primary WAN Connection): verificare che l'interfaccia non sia in stato shutdown. Selezionare valori di dispositivo specifici per il nome dell'interfaccia, la descrizione e l'indirizzo IP:

Cisco vManage Select Resource Group Configuration - Templates

Device Feature

Feature Template > Add Template > VPN Interface Ethernet

Template Name Site35_VPN_Interface_Ethernet
Description Primary WAN Circuit

Basic Configuration Tunnel NAT VRRP ACL/QoS ARP 802.1X Advanced

BASIC CONFIGURATION

Shutdown Yes No

Interface Name [primary_wan_interface]

Description [primary_wan_interface_description]

IPv4 IPv6

Dynamic Static

IPv4 Address [primary_wan_interface_ip]

Secondary IP Address (Maximum: 4) Add

DHCP Helper

Block Non Source IP Yes No

Bandwidth Upstream

Bandwidth Downstream

Cancel Save

Configurazione base modello di funzionalità dell'interfaccia WAN primaria

Verificare che l'interfaccia del tunnel sia impostata su ON. Selezionare il valore del dispositivo specifico per il colore primario della WAN:

Feature Template > VPN Interface Ethernet > Site35_VPN_Interface_Ethernet

Basic Configuration Tunnel NAT VRRP ACL/QoS ARP 802.1X Advanced

TUNNEL

Tunnel Interface On Off

Per-tunnel Qos On Off

Color [primary_WAN_color_value]

Restrict On Off

Groups

Border On Off

Maximum Control Connections 1

vBond As Stun Server On Off

Exclude Controller Group List

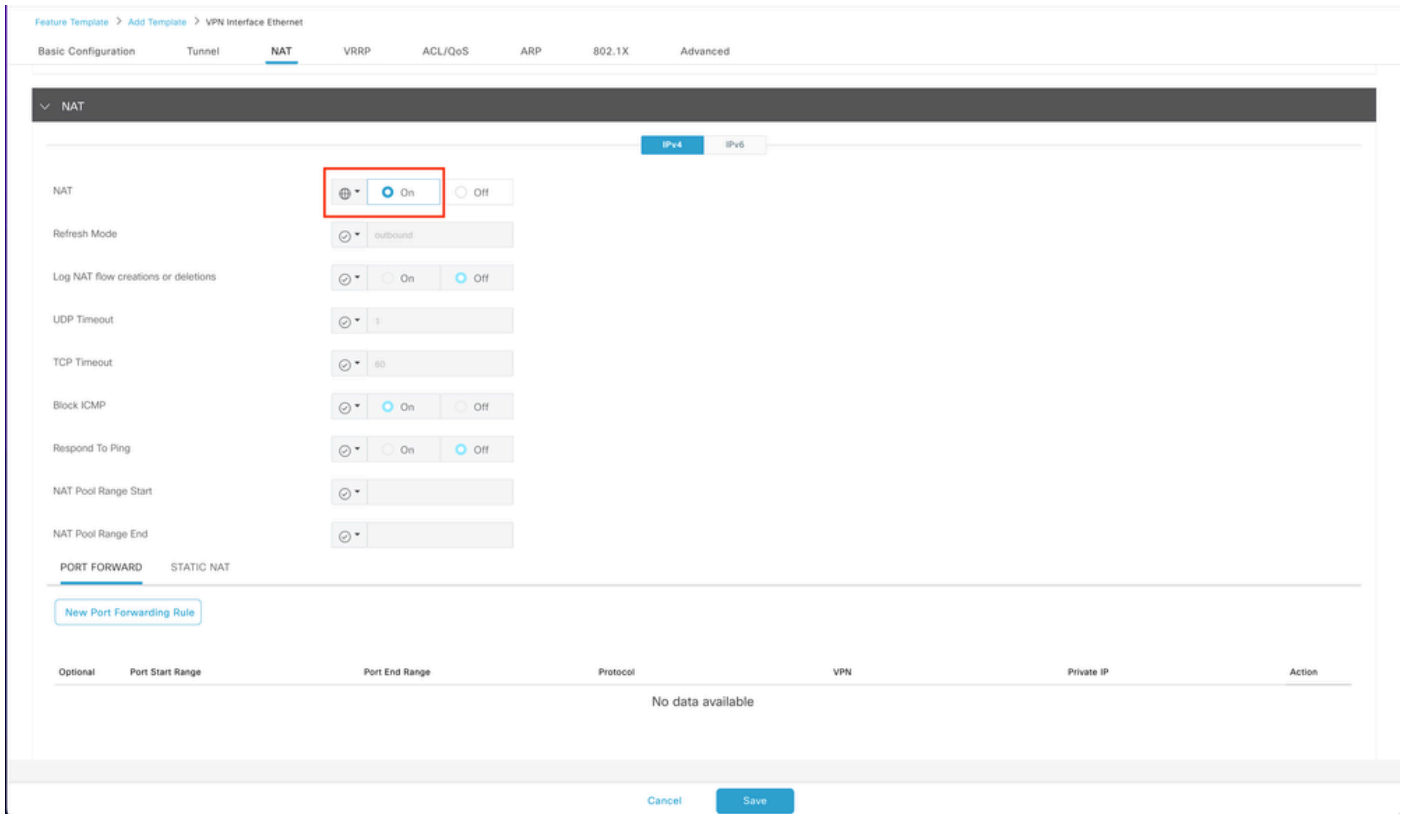
vManage Connection Preference 8

Port Hop On Off

Low-Bandwidth Link On Off

Interfaccia tunnel modello funzione VPN 0

Verificare che NAT sia impostato su ON per l'interfaccia WAN pubblica:



Modello di interfaccia VPN 0 NAT

3. VPN Interface Ethernet (TLOC-EXT/NO Tunnel Interface): verificare che l'interfaccia TLOC-Ext sia nello stato no shutdown. Selezionare i valori di periferica specifici per interfaccia, descrizione e indirizzo IP. Verificare che l'interfaccia tunnel sia impostata su Off:

Feature Template > VPN Interface Ethernet > Site35_TLOC_Ext_NoTunnel

Device Type: ISR 1100 6G (Viptela OS),ISR 1100X 6G (Viptela OS),ISR 1100 4GLTE* (Viptela OS),ISR 1100 4G (Viptela OS),ISR 1100X 4G (Viptela OS)

Template Name: Site35_TLOC_Ext_NoTunnel

Description: Site 35 TLOC Extension Template without Tunnel Config

Basic Configuration | Tunnel | NAT | VRRP | ACL/QoS | ARP | 802.1X | Advanced

BASIC CONFIGURATION

Shutdown: Yes No

Interface Name: [TLOC_NoTunnel_Interface]

Description: [TLOC_NoTunnel_Interface_Description]

IPv4 IPv6

Dynamic Static

IPv4 Address: [TLOC_NoTunnel_Interface_IP]

Secondary IP Address (Maximum: 4): [Add](#)

DHCP Helper:

Block Non Source IP: Yes No

Bandwidth Upstream:

Bandwidth Downstream:

TUNNEL

Tunnel Interface: On Off

Cancel Update

Configurazione base interfaccia tunnel TLOC-EXT/NO

Add TLOC-Ext interface in Advanced Section (Aggiungi interfaccia TLOC-Ext nella sezione avanzata):

Feature Template > VPN Interface Ethernet > Site35_TLOC_Ext_NoTunnel

Basic Configuration Tunnel NAT VRRP ACL/QoS ARP 802.1X **Advanced**

ADVANCED

Duplex	<input type="text"/>
MAC Address	<input type="text"/>
IP MTU	<input type="text" value="1500"/>
PMTU Discovery	<input type="radio"/> On <input checked="" type="radio"/> Off
Flow Control	<input type="text" value="autoneg"/>
TCP MSS	<input type="text"/>
Speed	<input type="text"/>
Clear-Dont-Fragment	<input type="radio"/> On <input checked="" type="radio"/> Off
Static Ingress QoS	<input type="text"/>
ARP Timeout	<input type="text" value="1200"/>
Autonegotiation	<input checked="" type="radio"/> On <input type="radio"/> Off
TLOC Extension	<input type="text" value="ge0/0"/>
Tracker	<input type="text"/>
ICMP/ICMPv6 Redirect Disable	<input type="radio"/> On <input checked="" type="radio"/> Off
GRE tunnel source IP	<input type="text"/>
Xconnect	<input type="text"/>
IP Directed-Broadcast	<input type="radio"/> On <input checked="" type="radio"/> Off

Interfaccia TLOC-Ext

4. VPN Interface Ethernet (Tunnel Interface/No Tloc-ext): verificare che l'interfaccia non sia in stato shutdown. Selezionare i valori di periferica specifici per interfaccia, descrizione e indirizzo IP:

Device Type: ISR 1100 4G (Viptela OS),ISR 1100 4GLTE* (Viptela OS),ISR 1100 6G (Viptela OS),ISR 1100X 4G (Viptela OS),ISR 1100X 6G (Viptela OS)

Template Name: Site35_Tunnel_NoTlocExt

Description: Site 35 TLOC Tunnel Configuration No TLOC-Ext

Basic Configuration | Tunnel | NAT | VRRP | ACL/QoS | ARP | 802.1X | Advanced

▼ BASIC CONFIGURATION

Shutdown: Yes No

Interface Name: [dropdown] [interface_tunn_notlocext]

Description: [dropdown] [interface_description_tunn_notlocext]

IPv4 IPv6

Dynamic Static

IPv4 Address: [dropdown] [interface_ip_tunn_notlocext]

Secondary IP Address (Maximum: 4): [Add](#)

DHCP Helper: [dropdown]

Interfaccia tunnel/Nessuna configurazione Tloc-ext Basic

Verificare che l'interfaccia del tunnel sia impostata su ON. Selezionare il valore di periferica specifico per il colore Tloc-Ext:

Device Feature

Feature Template > Add Template > VPN Interface Ethernet

Basic Configuration Tunnel NAT VRRP ACL/QoS ARP 802.1X Advanced

▼ TUNNEL

Tunnel Interface On Off

Per-tunnel Qos On Off

Color [flocext_color_value]

Restrict On Off

Groups

Border On Off

Maximum Control Connections

vBond As Stun Server On Off

Exclude Controller Group List

vManage Connection Preference 5

Port Hop On Off

Low-Bandwidth Link On Off

Interfaccia tunnel

Modello dispositivo

Passaggi per la creazione del modello di dispositivo:

1. Creare il modello di dispositivo dal modello di funzionalità:

Cisco vManage Select Resource Group Configuration · Templates

Device Feature

Search

Create Template

From Feature Template

CLI Template

Total Rows: 0

Name	Description	Type	Device Model	Device Role	Resource Group	Feature Templates	Draft Mode	Devices Attached	Updated By	Last Updated	Template Status
No data available											

Modello di dispositivo da modello funzionalità

2. Inserire tutti i modelli di feature richiesti:

Device Feature

Device Model: ISR 1100 4G LTE* (Viptela OS)

Device Role: SDWAN Edge

Template Name: Site35_FeatureTemplate

Description: Template used for Site 35

Basic Information Transport & Management VPN Service VPN Cellular Additional Templates

Basic Information

System * Site35_System Additional System Templates

Logging* Site35_Logging

NTP Site35_NTP

AAA Site35_AAA BFD * Site35_BFD OMP * Site35_OMP

Security * Site35_Security

Dettagli modello dispositivo con configurazione di base dei modelli di funzionalità

Cisco vManage Select Resource Group Configuration - Templates

Device Feature

Basic Information Transport & Management VPN Service VPN Cellular Additional Templates

Transport & Management VPN

VPN 0 * Site35_VPN0 Additional VPN 0 Templates

VPN Interface Site35_VPN_Interface_Ethernet

VPN Interface Site35_TLOC_Ext_NoTunnel

VPN Interface Site35_Tunnel_NoTlocExt

VPN 512 * Site35_VPN512 Additional VPN 512 Templates

Dettagli del modello di dispositivo con i modelli di funzionalità Trasporto e gestione

3. Collegare entrambi i dispositivi al modello di dispositivo:

Cisco vManage Select Resource Group Configuration - Templates

Device Feature

Q Search

Create Template v

Template Type Non-Default v

Total Rows: 1

Name	Description	Type ...	Device Model	Device Role ...	Resource Group	Feature Templates	Draft Mode	Devices Attached	Updated By	Last Updated	Template Status
Site35_FeatureTemplate	Template used ...	Feature	ISR 1100 4G LTE* (Viptela OS)	SDWAN Edge	global	12	Disabled	0	admin	25 Jul 2022 12:2...	In Sync

- Edit
- View
- Delete
- Copy
- Attach Devices
- Change Resource Group
- Export CSV

Collegare dispositivi ai modelli

4. Spostare entrambe le periferiche dalla scheda Periferiche disponibili alla scheda Periferiche selezionate:

Attach Devices

Attach device from the list below

Available Devices

All

Name	Device IP
------	-----------

Selected Devices 2 Items Selected Select All

All

Name	Device IP
vEdge	10.10.10.17
vEdge	10.10.10.19

Sposta dispositivi da disponibili a selezionati

5. Inserire tutti i dettagli richiesti per entrambi i dispositivi:

Sito35_vEdge1

Update Device Template



Variable List (Hover over each field for more information)

Status	complete
Chassis Number	ISR1100-4GLTEGB-FGL2347LHT6
System IP	10.10.10.17
Hostname	vEdge
Name(vpn0_name)	<input type="text" value="Transport"/>
Address(primary_WAN_next_hop)	<input type="text" value="10.201.237.1"/>
Address(tlocext_nexthop)	<input type="text" value="192.168.30.5"/>
Interface Name(interface_tunn_notlocext)	<input type="text" value="ge0/1"/>
Description(interface_description_tunn_notlocext)	<input type="text" value="TunnellInterface_NoTLOCExt"/>
IPv4 Address(interface_ip_tunn_notlocext)	<input type="text" value="192.168.30.4/24"/>
Color(tlocext_color_value)	<input type="text" value="private2"/>
Interface Name(TLOC_NoTunnel_Interface)	<input type="text" value="ge0/2"/>
Description(TLOC_NoTunnel_Interface_Description)	<input type="text" value="TLOC_NoTunnellInterface"/>
IPv4 Address(TLOC_NoTunnel_Interface_IP)	<input type="text" value="192.168.40.4/24"/>
Interface Name(primary_wan_interface)	<input type="text" value="ge0/0"/>
Description(primary_wan_interface_description)	<input type="text" value="Primary WAN connection"/>
IPv4 Address(primary_wan_interface_IP)	<input type="text" value="10.201.237.120/24"/>
Color(primary_WAN_color_value)	<input type="text" value="private1"/>
Hostname(system_host_name)	<input type="text" value="Site35_vEdge1"/>
System IP(system_system_ip)	<input type="text" value="10.10.10.17"/>
Site ID(system_site_id)	<input type="text" value="35"/>

[Generate Password](#)

[Update](#)

[Cancel](#)

Aggiorna valori 1

Sito35_vEdge2



Update Device Template

Variable List (Hover over each field for more information)

Status	complete
Chassis Number	ISR1100-4GLTENA-FGL2347LJ1G
System IP	10.10.10.19
Hostname	vEdge
Name(vpn0_name)	<input type="text" value="Transport"/>
Address(primary_WAN_next_hop)	<input type="text" value="10.201.237.1"/>
Address(tlocext_nexthop)	<input type="text" value="192.168.40.4"/>
Interface Name(interface_tunn_notlocext)	<input type="text" value="ge0/2"/>
Description(interface_description_tunn_notlocext)	<input type="text" value="TunnelInterface_NoTLOCExt"/>
IPv4 Address(interface_ip_tunn_notlocext)	<input type="text" value="192.168.40.5/24"/>
Color(tlocext_color_value)	<input type="text" value="private1"/>
Interface Name(TLOC_NoTunnel_Interface)	<input type="text" value="ge0/1"/>
Description(TLOC_NoTunnel_Interface_Description)	<input type="text" value="TLOC_NoTunnelInterface"/>
IPv4 Address(TLOC_NoTunnel_Interface_IP)	<input type="text" value="192.168.30.5/24"/>
Interface Name(primary_wan_interface)	<input type="text" value="ge0/0"/>
Description(primary_wan_interface_description)	<input type="text" value="Primary WAN connection"/>
IPv4 Address(primary_wan_interface_IP)	<input type="text" value="10.201.237.66/24"/>
Color(primary_WAN_color_value)	<input type="text" value="private2"/>
Hostname(system_host_name)	<input type="text" value="Site35_vEdge2"/>
System IP(system_system_ip)	<input type="text" value="10.10.10.19"/>
Site ID(system_site_id)	<input type="text" value="35"/>

Generate Password

Update

Cancel

Aggiorna valori 2

6. Verificare che i valori selezionati siano destinati ai seguenti dispositivi:

Sito35_vEdge1

Cisco vManage Configuration - Templates

Device Template	Total	76	allow-service sshd	78	allow-service sshd
Site35_FeatureTemplate	1	77	no allow-service netconf	79	no allow-service netconf
		78	no allow-service ntp	80	no allow-service ntp
		79	no allow-service ospf	81	no allow-service ospf
		80	no allow-service stun	82	no allow-service stun
		81	allow-service https	83	allow-service https
		82	:	84	:
		83	no shutdown	85	no shutdown
		84	:	86	:
				87	interface ge0/1
				88	description TunnelInterface_NoTLOCExt
				89	ip address 192.168.30.4/24
				90	tunnel-interface
				91	encapsulation ipsec
				92	color private2
				93	max-control-connections 1
				94	no allow-service bgp
				95	allow-service dhcp
				96	allow-service dns
				97	allow-service icmp
				98	no allow-service sshd
				99	no allow-service netconf
				100	no allow-service ntp
				101	no allow-service ospf
				102	no allow-service stun
				103	allow-service https
				104	:
				105	no shutdown
				106	:
				107	interface ge0/2
				108	description TLOC_NoTunnelInterface
				109	ip address 192.168.40.4/24
				110	no shutdown
				111	:
				112	ip route 0.0.0.0/0 10.201.237.1 1
				113	ip route 0.0.0.0/0 192.168.30.5 1
				114	:
				115	vpn 512
				116	:
				117	:
				118	:
				119	:

Back Configure Devices Cancel

Anteprima configurazione 1

Sito35_vEdge2

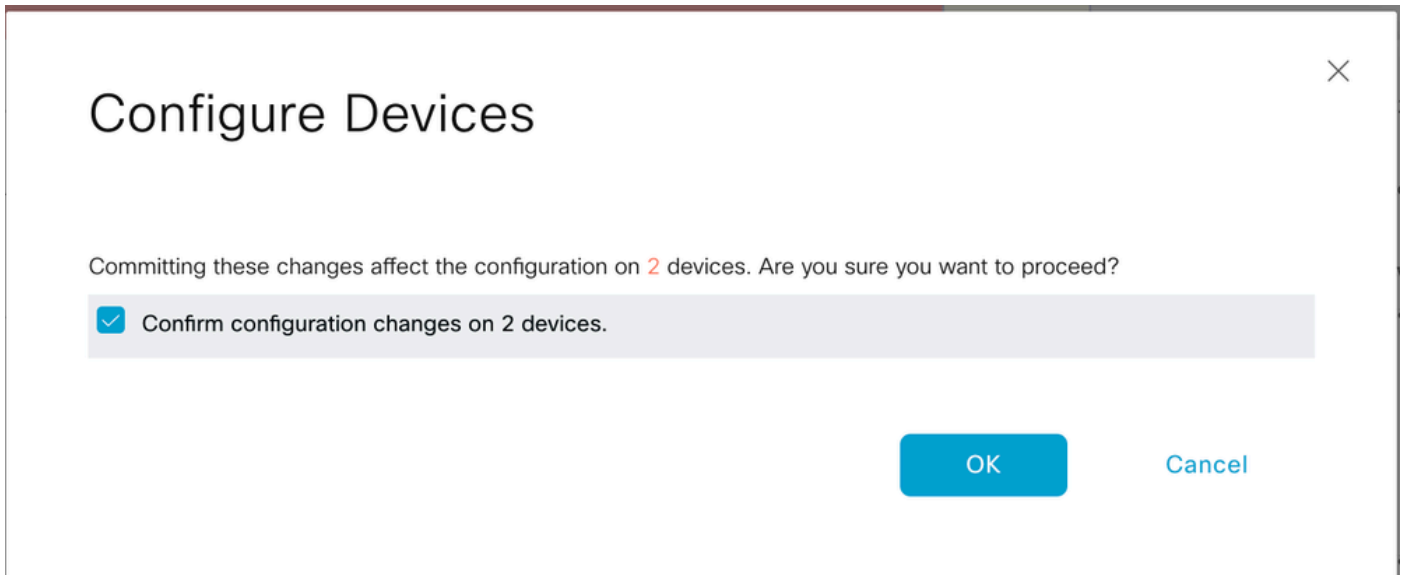
Cisco vManage Configuration - Templates

Device Template	Total	75	allow-service sshd	78	allow-service sshd
Site35_FeatureTemplate	1	76	no allow-service netconf	79	no allow-service netconf
		77	no allow-service ntp	80	no allow-service ntp
		78	no allow-service ospf	81	no allow-service ospf
		79	no allow-service stun	82	no allow-service stun
		80	allow-service https	83	allow-service https
		81	:	84	:
		82	no shutdown	85	no shutdown
		83	:	86	:
				87	interface ge0/1
				88	description TLOC_NoTunnelInterface
				89	ip address 192.168.30.5/24
				90	no shutdown
				91	:
				92	interface ge0/2
				93	description TunnelInterface_NoTLOCExt
				94	ip address 192.168.40.5/24
				95	tunnel-interface
				96	encapsulation ipsec
				97	color private1
				98	max-control-connections 1
				99	no allow-service bgp
				100	allow-service dhcp
				101	allow-service dns
				102	allow-service icmp
				103	no allow-service sshd
				104	no allow-service netconf
				105	no allow-service ntp
				106	no allow-service ospf
				107	no allow-service stun
				108	allow-service https
				109	:
				110	no shutdown
				111	:
				112	ip route 0.0.0.0/0 10.201.237.1 1
				113	ip route 0.0.0.0/0 192.168.40.4 1
				114	:
				115	vpn 512
				116	:
				117	:
				118	:
				119	:

Back Configure Devices Cancel

Anteprima configurazione 2

6. Infine, spingere la configurazione sul dispositivo:



Conferma configurazione

L'output successivo acquisisce la configurazione in esecuzione per vpn 0 una volta che il push del modello è riuscito:

Sito35_vEdge1

```
Site35_vEdge1# show run vpn 0
vpn 0
interface ge0/0
ip address 10.201.237.120/24
ipv6 dhcp-client
nat
!
tunnel-interface
encapsulation ipsec
color private1
max-control-connections 1
no allow-service bgp
allow-service dhcp
allow-service dns
allow-service icmp
allow-service sshd
no allow-service netconf
no allow-service ntp
no allow-service ospf
no allow-service stun
allow-service https
!
no shutdown
!
interface ge0/1
description TunnelInterface_NoTLOExt
ip address 192.168.30.4/24
tunnel-interface
encapsulation ipsec
color private2
max-control-connections 1
no allow-service bgp
allow-service dhcp
```



```
allow-service dns
allow-service icmp
no allow-service sshd
no allow-service netconf
no allow-service ntp
no allow-service ospf
no allow-service stun
allow-service https
!
no shutdown
!
interface ge0/2
description TL0C_NoTunnelInterface
ip address 192.168.40.4/24
tloc-extension ge0/0
no shutdown
!

ip route 0.0.0.0/0 10.201.237.1
ip route 0.0.0.0/0 192.168.30.5
!
Site35_vEdge1#
```

Sito35_vEdge2

```
Site35_vEdge2#
Site35_vEdge2#
Site35_vEdge2#
Site35_vEdge2# sh run vpn 0
vpn 0
interface ge0/0
ip address 10.201.237.66/24
ipv6 dhcp-client
nat
!
tunnel-interface
encapsulation ipsec
color private2
max-control-connections 1
no allow-service bgp
allow-service dhcp
allow-service dns
allow-service icmp
allow-service sshd
no allow-service netconf
no allow-service ntp
no allow-service ospf
no allow-service stun
allow-service https
!
no shutdown
!
interface ge0/1
description TL0C_NoTunnelInterface
ip address 192.168.30.5/24
tloc-extension ge0/0
no shutdown
!
```

```

interface ge0/2
description TunnelInterface_NoTLOCExt
ip address 192.168.40.5/24
tunnel-interface
encapsulation ipsec
color private1
max-control-connections 1
no allow-service bgp
allow-service dhcp
allow-service dns
allow-service icmp
no allow-service sshd
no allow-service netconf
no allow-service ntp
no allow-service ospf
no allow-service stun
allow-service https
!
no shutdown
!
ip route 0.0.0.0/0 10.201.237.1
ip route 0.0.0.0/0 192.168.40.4
!
Site35_vEdge2#

```

Verifica

1. Il modello è stato collegato correttamente a entrambi i dispositivi:

Push Feature Template Configuration ● Validation Success Initiated By: admin From: 10.24.227.28

Total Task: 2 | Success: 2

Search Total Rows: 2

Status	Message	Chassis Number	Device Model	Hostname	System IP	Site ID	vManage IP
● Success	Done - Push Feature Template Con...	ISR1100-4GLTEGB-FGL2347LHT6	ISR 1100 4GLTE* (Viptela OS)	vEdge	10.10.10.17	35	10.10.10.1
<pre> [25-Jul-2022 18:16:20 UTC] Checking and creating device in vManage [25-Jul-2022 18:16:21 UTC] Generating configuration from template [25-Jul-2022 18:16:27 UTC] Device is online [25-Jul-2022 18:16:27 UTC] Updating device configuration in vManage [25-Jul-2022 18:16:27 UTC] Sending configuration to device [25-Jul-2022 18:16:40 UTC] Completed template push to device. [25-Jul-2022 18:16:41 UTC] Template successfully attached to device </pre>							
● Success	Done - Push Feature Template Con...	ISR1100-4GLTENA-FGL2347LJ1G	ISR 1100 4GLTE* (Viptela OS)	vEdge	10.10.10.19	35	10.10.10.1
<pre> [25-Jul-2022 18:16:20 UTC] Checking and creating device in vManage [25-Jul-2022 18:16:20 UTC] Generating configuration from template [25-Jul-2022 18:16:26 UTC] Device is online [25-Jul-2022 18:16:26 UTC] Updating device configuration in vManage [25-Jul-2022 18:16:27 UTC] Sending configuration to device [25-Jul-2022 18:16:38 UTC] Completed template push to device. [25-Jul-2022 18:16:41 UTC] Template successfully attached to device </pre>							

Push del modello riuscito

2. La connessione di controllo è attiva tramite la WAN primaria e l'interfaccia TLOC-Ext:

```
Site35_vEdge1# show control connections
```

PEER TYPE	PEER PROT	PEER SYSTEM IP	SITE ID	DOMAIN ID	PEER PRIVATE IP	PEER PRIV PORT	PEER PUBLIC IP	PEER PUB PORT	ORGANIZATION	LOCAL COLOR	CONTROLLER GROUP PROXY	STATE	UPTIME	ID
vsmart	dtls	10.10.10.3	1	1	10.201.237.137	12446	10.201.237.137	12446	rcdn_sdwan_lab	private1	No	up	0:00:01:47	0
vsmart	dtls	10.10.10.3	1	1	10.201.237.137	12446	10.201.237.137	12446	rcdn_sdwan_lab	private2	No	up	0:00:01:42	0
vmanage	dtls	10.10.10.1	1	0	10.201.237.91	12446	10.201.237.91	12446	rcdn_sdwan_lab	private1	No	up	0:00:01:52	0

```
Site35_vEdge1#
```

Verifica connessione di controllo 1

```
Site35_vEdge2# show control connections
```

PEER TYPE	PEER PROT	PEER SYSTEM IP	SITE ID	DOMAIN ID	PEER PRIVATE IP	PEER PRIV PORT	PEER PUBLIC IP	PEER PUB PORT	LOCAL COLOR	PROXY	STATE	UPTIME	CONTROLLER GROUP ID
vsmart	dtls	10.10.10.3	1	1	10.201.237.137	12446	10.201.237.137	12446	private2	No	up	0:00:00:25	0
vsmart	dtls	10.10.10.3	1	1	10.201.237.137	12446	10.201.237.137	12446	private1	No	up	0:00:00:15	0
vmanage	dtls	10.10.10.1	1	0	10.201.237.91	12446	10.201.237.91	12446	private2	No	up	0:00:00:20	0

Verifica connessione di controllo 2

Scenari d'uso

A seconda della progettazione del sito locale, l'estensione TLOC può essere implementata anche utilizzando l'estensione L2 o L3 TLOC.

1. Estensione TLOC L2: queste estensioni si trovano nello stesso dominio di broadcast o nella stessa subnet.
2. Estensione L3 TLOC: Queste estensioni sono separate da un dispositivo L3 e possono eseguire qualsiasi protocollo di routing (è supportato solo sui dispositivi Cisco IOSXE SD-WAN)



Nota: vedere la sezione TLOC Extension nel capitolo WAN Edge Deployment della [Cisco SD-WAN Design Guide](#).

Limitazioni

- Le interfacce di estensione TLOC e TLOC sono supportate solo sulle interfacce con routing L3. Gli switchport/SVI L2 non possono essere utilizzati come interfacce WAN/Tunnel e possono essere utilizzati solo sul lato servizio.
- Anche l'LTE non viene usato come interfaccia di estensione TLOC tra router WAN Edge.
- L3 Estensione TLOC è supportata solo sui router Cisco IOSXE SD-WAN e non sui router vEdge.
- L'estensione TLOC non funziona sulle interfacce di trasporto associate alle interfacce del tunnel di loopback.

Informazioni correlate

- [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).