

Konfigurieren der TLOC-Erweiterung mithilfe der vManage-Funktionsvorlage

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Netzwerkdiagramm](#)

[Konfigurationen](#)

[VPN-Funktionsvorlage](#)

[Gerätevorlage](#)

[Verifizierung](#)

[Anwendungsfälle](#)

[Einschränkungen](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie die TLOC-Erweiterung mithilfe der vManage-Funktionsvorlage konfigurieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Verwendung der vManage-Funktionsvorlage
- Zwei (2) vEdge-Geräte müssen erfolgreich in vManage integriert werden.

Verwendete Komponenten

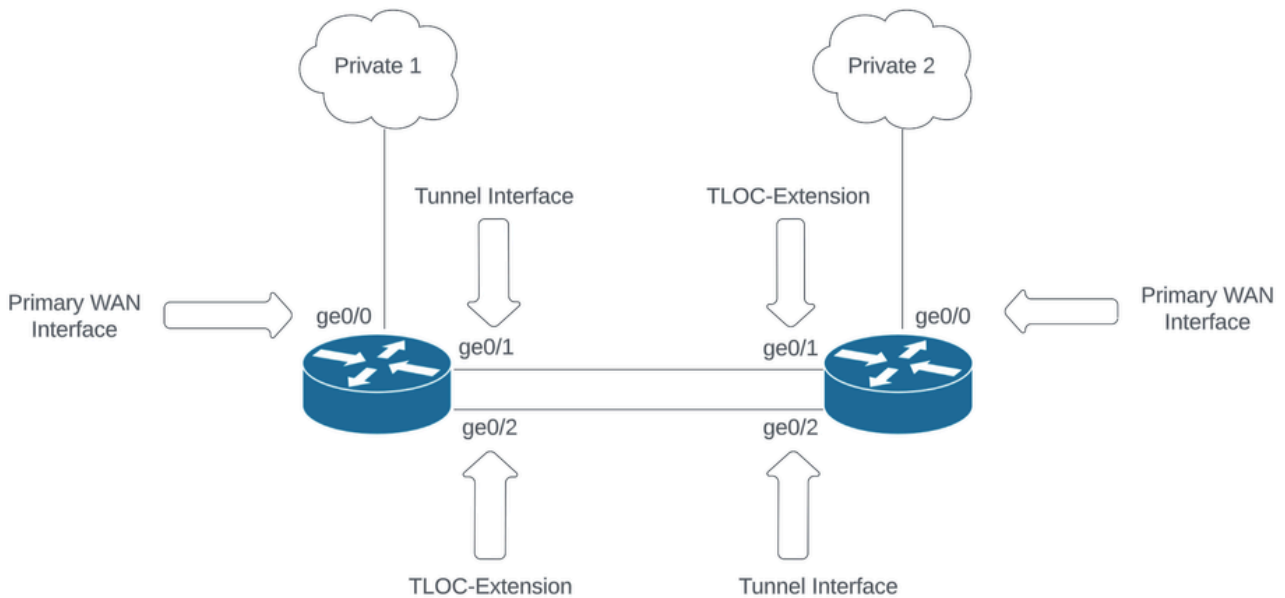
Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco vManage, Version 20.6.3
- vEdge 20.6.3

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.

Netzwerkdiagramm



Netzwerktopologie

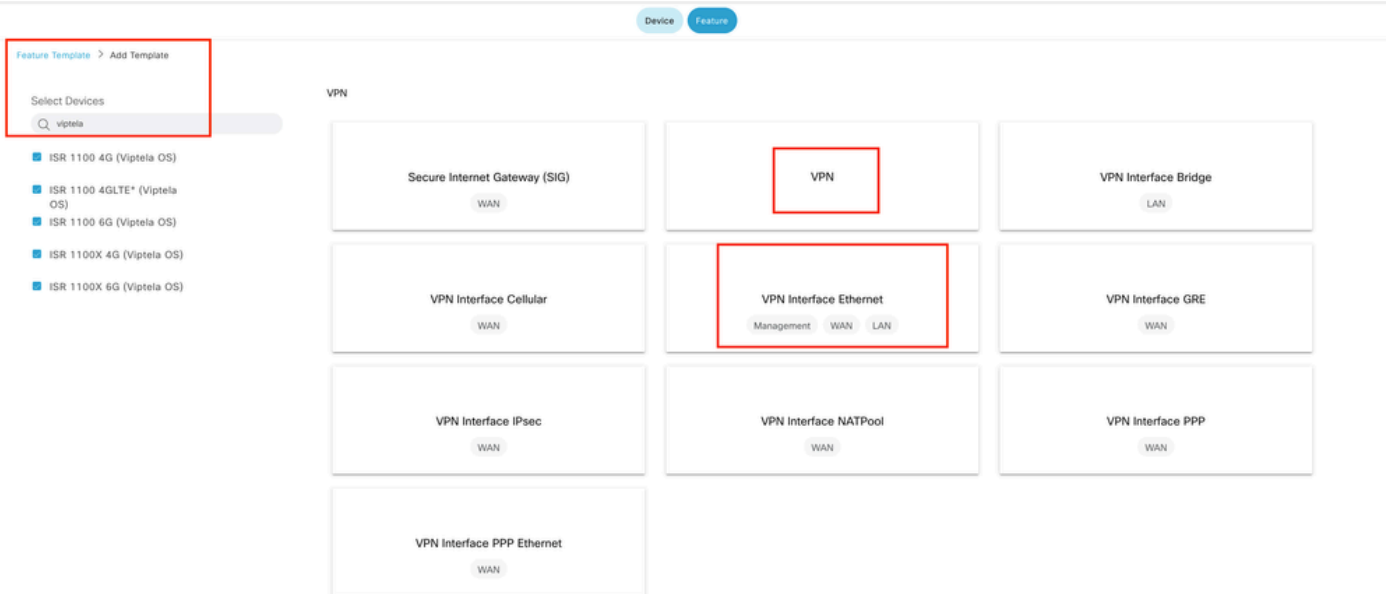
Konfigurationen

In diesem Dokument wird davon ausgegangen, dass Sie bereits die restlichen Funktionsvorlagen konfiguriert haben. Derselbe Workflow für Funktionsvorlagen gilt für Cisco IOS® XE SD-WAN-Geräte.

Erstellen Sie insgesamt vier Funktionsvorlagen, die auf die vEdge-Gerätevorlage angewendet werden sollen.

VPN-Funktionsvorlage

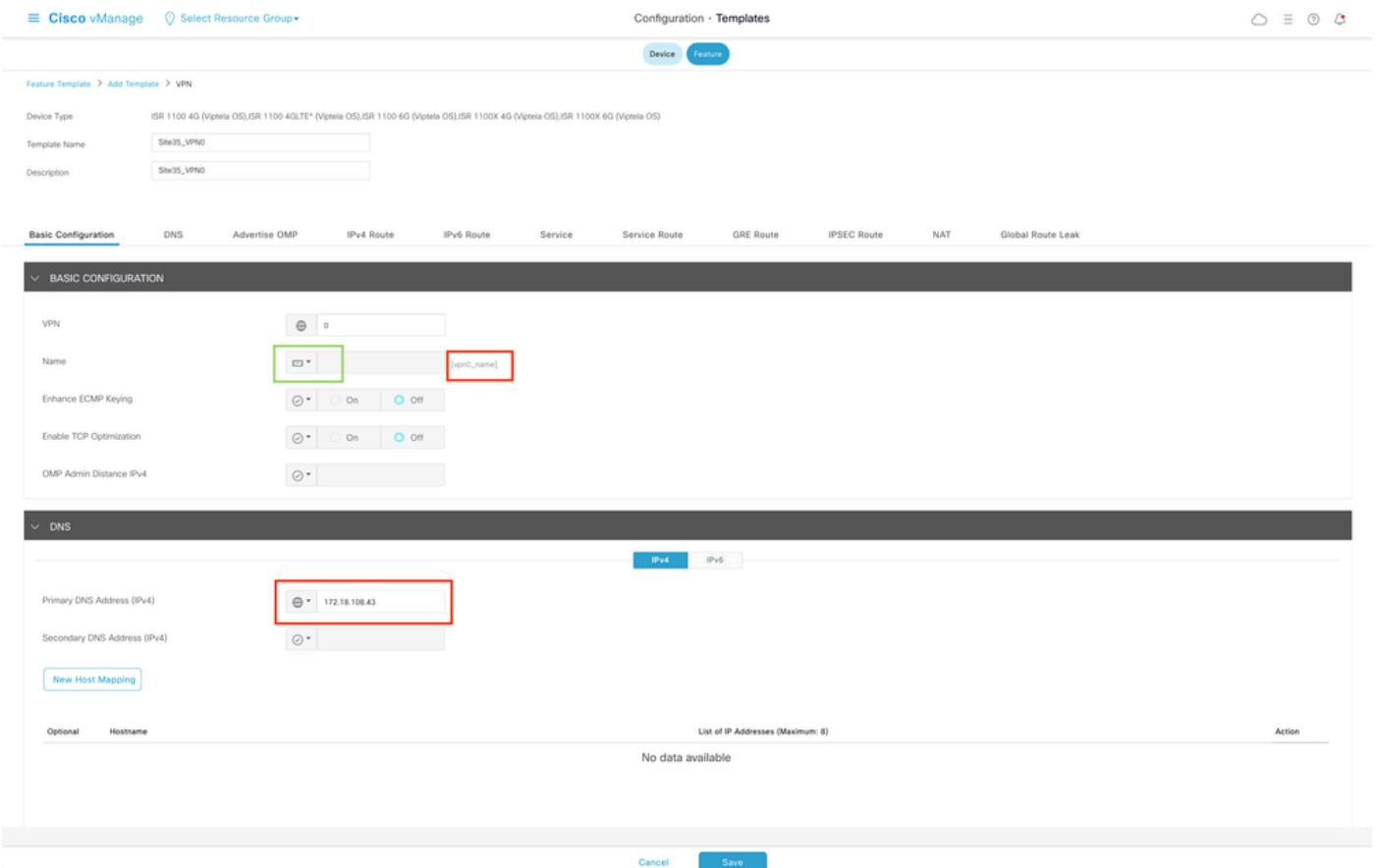
Diese Funktionsvorlage umfasst VPN 0, VPN Interface Ethernet (primäre WAN-Verbindung), VPN Interface Ethernet (Tunnel/NoTlocExt) und VPN Interface Ethernet (TlocExt/NoTunnel):



VPN-Funktionsvorlagen

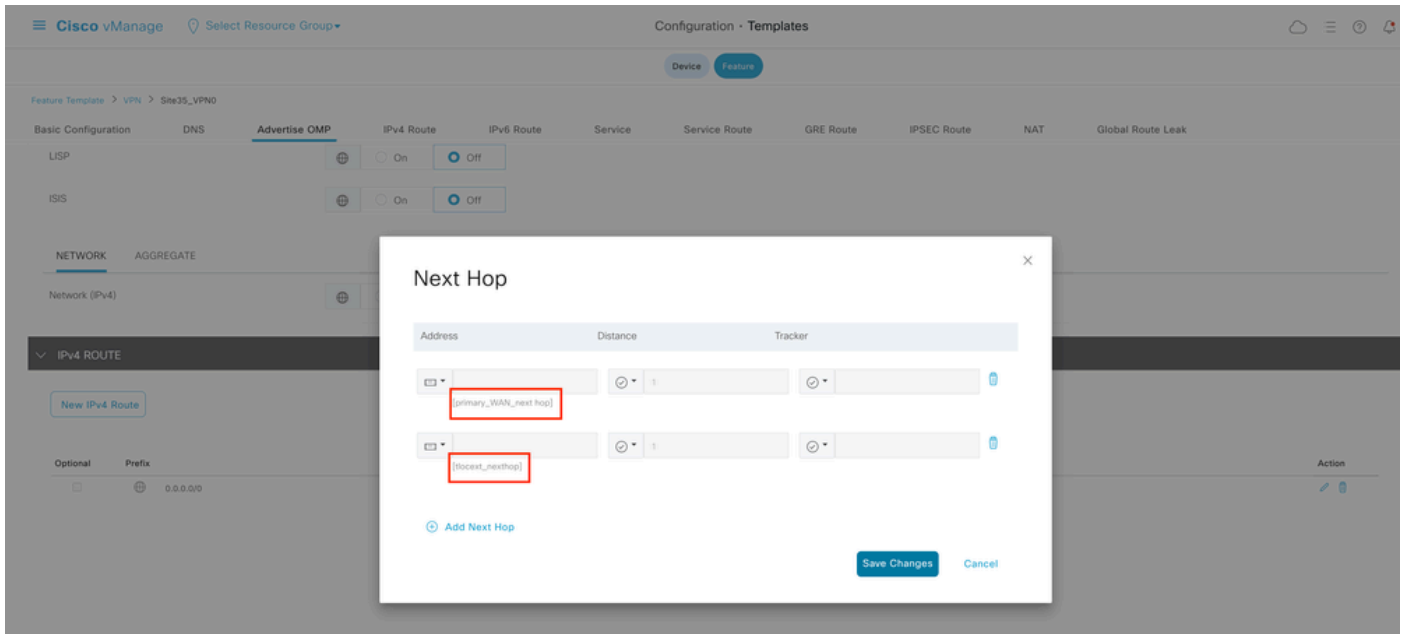
Schritte zum Erstellen von Funktionsvorlagen:

1. VPN 0: Wählen Sie im Abschnitt für die Basiskonfiguration den spezifischen Gerätewert für Transport-VPN aus, und fügen Sie die DNS-Serveradresse im Abschnitt für DNS hinzu:

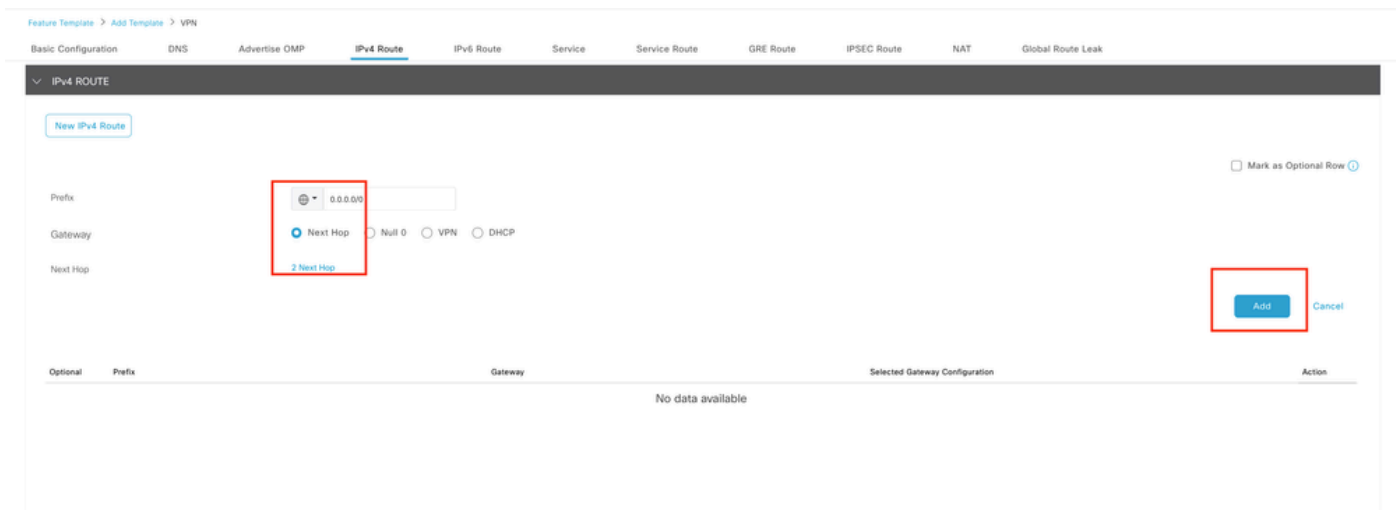


Grundlegende Konfiguration der VPN 0-Funktionsvorlage

Fügen Sie im IPv4-Routenabschnitt ein Präfix mit spezifischen Gerätewerten für zwei Next-Hop-Adressen (primäres WAN und TLOC-EXT) hinzu:



VPN 0-Funktionsvorlage - IPv4-Route



VPN 0-Funktionsvorlage - IPv4-Route Next-Hop

2. VPN-Schnittstellen-Ethernet (primäre WAN-Verbindung): Stellen Sie sicher, dass sich die Schnittstelle in keinem heruntergefahrenen Zustand befindet. Wählen Sie bestimmte Gerätewerte für Schnittstellennamen, Beschreibung und IP-Adresse aus:

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

Feature-Vorlage für primäre WAN-Schnittstelle Grundkonfiguration

Stellen Sie sicher, dass die Tunnelschnittstelle auf ON eingestellt ist. Wählen Sie den spezifischen Gerätewert für die primäre WAN-Farbe aus:

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

VPN 0-Funktionsvorlage - Tunnelschnittstelle

Stellen Sie sicher, dass NAT für die öffentliche WAN-Schnittstelle EIN ist:

Feature Template > Add Template > VPN Interface Ethernet

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

IPv4 IPv6

NAT On Off

Refresh Mode inbound outbound

Log NAT flow creations or deletions On Off

UDP Timeout 1

TCP Timeout 60

Block ICMP On Off

Respond To Ping On Off

NAT Pool Range Start

NAT Pool Range End

PORT FORWARD STATIC NAT

New Port Forwarding Rule

Optional	Port Start Range	Port End Range	Protocol	VPN	Private IP	Action
No data available						

Cancel Save

NAT-Vorlage für VPN 0-Schnittstelle

3. VPN-Schnittstellen-Ethernet (TLOC-EXT/NO Tunnel Interface): Stellen Sie sicher, dass sich die TLOC-Ext-Schnittstelle im nicht heruntergefahrenen Zustand befindet. Wählen Sie die spezifischen Gerätewerte für Schnittstelle, Beschreibung und IP-Adresse aus. Stellen Sie sicher, dass die Tunnelschnittstelle auf Aus eingestellt ist:

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

TLOC-EXT/NO Tunnelschnittstelle Grundkonfiguration

Hinzufügen einer TLOC-Ext-Schnittstelle im erweiterten Abschnitt:

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

TLOC-Ext-Schnittstelle

4. VPN Interface Ethernet (Tunnel Interface/No Tloc-ext): Stellen Sie sicher, dass sich die Schnittstelle im nicht heruntergefahrenen Zustand befindet. Wählen Sie die spezifischen Gerätewerte für Schnittstelle, Beschreibung und IP-Adresse aus:

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]

Dynamic Static

IPv4 Address: [dropdown] [interface_ip_tunn_notlocext]

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

DHCP Helper: [dropdown]

IPv4 | IPv6

Tunnelschnittstelle/Kein Tloc-ext Basiskonfiguration

Stellen Sie sicher, dass die Tunnelschnittstelle auf ON eingestellt ist. Wählen Sie den spezifischen Gerätewert für die Farbe "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

Tunnelschnittstelle

Gerätevorlage

Schritte zum Erstellen der Gerätevorlage:

1. Erstellen Sie die Gerätevorlage aus der KE-Vorlage:

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											

Gerätevorlage aus Funktionsvorlage

2. Füllen Sie alle erforderlichen Funktionsvorlagen aus:

Device Feature

Device Model: ISR 1100 4G LTE* (Vipteta 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

Details zu Gerätevorlagen mit der Basiskonfiguration von Funktionsvorlagen

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

Details zu Gerätevorlagen mit Funktionsvorlagen Transport und Management

3. Verknüpfen Sie beide Geräte mit der Gerätevorlage:

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* (Vipteta 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

Hinzufügen von Geräten zu Vorlagen

4. Verschieben Sie beide Geräte von verfügbaren Geräten auf die Registerkarte "Ausgewählte Geräte":

Attach Devices ×

Attach device from the list below

Available Devices

All

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

>

<

2 Items Selected Select All

All

Name	Device IP
vEdge	10.10.10.17
vEdge	10.10.10.19

Attach Cancel

Verschieben von Geräten von verfügbar nach ausgewählt

5. Geben Sie alle erforderlichen Details für beide Geräte ein:

Standort35_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

Werte aktualisieren 1

Standort35_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)	Transport
Address(primary_WAN_next_hop)	10.201.237.1
Address(tlocext_nexthop)	192.168.40.4
Interface Name(interface_tunn_notlocext)	ge0/2
Description(interface_description_tunn_notlocext)	TunnelInterface_NoTLOCExt
IPv4 Address(interface_ip_tunn_notlocext)	192.168.40.5/24
Color(tlocext_color_value)	private1
Interface Name(TLOC_NoTunnel_Interface)	ge0/1
Description(TLOC_NoTunnel_Interface_Description)	TLOC_NoTunnelInterface
IPv4 Address(TLOC_NoTunnel_Interface_IP)	192.168.30.5/24
Interface Name(primary_wan_interface)	ge0/0
Description(primary_wan_interface_description)	Primary WAN connection
IPv4 Address(primary_wan_interface_IP)	10.201.237.66/24
Color(primary_WAN_color_value)	private2
Hostname(system_host_name)	Site35_vEdge2
System IP(system_system_ip)	10.10.10.19
Site ID(system_site_id)	35

Generate Password

Update

Cancel

Werte aktualisieren 2

6. Überprüfen Sie, ob die ausgewählten Werte für die folgenden Geräte bestimmt sind:

Standort35_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	!

Configure Device Rollback Timer

Back Configure Devices Cancel

Konfigurationsvorschau 1

Standort35_vEdge2

Cisco vManage Configuration - Templates

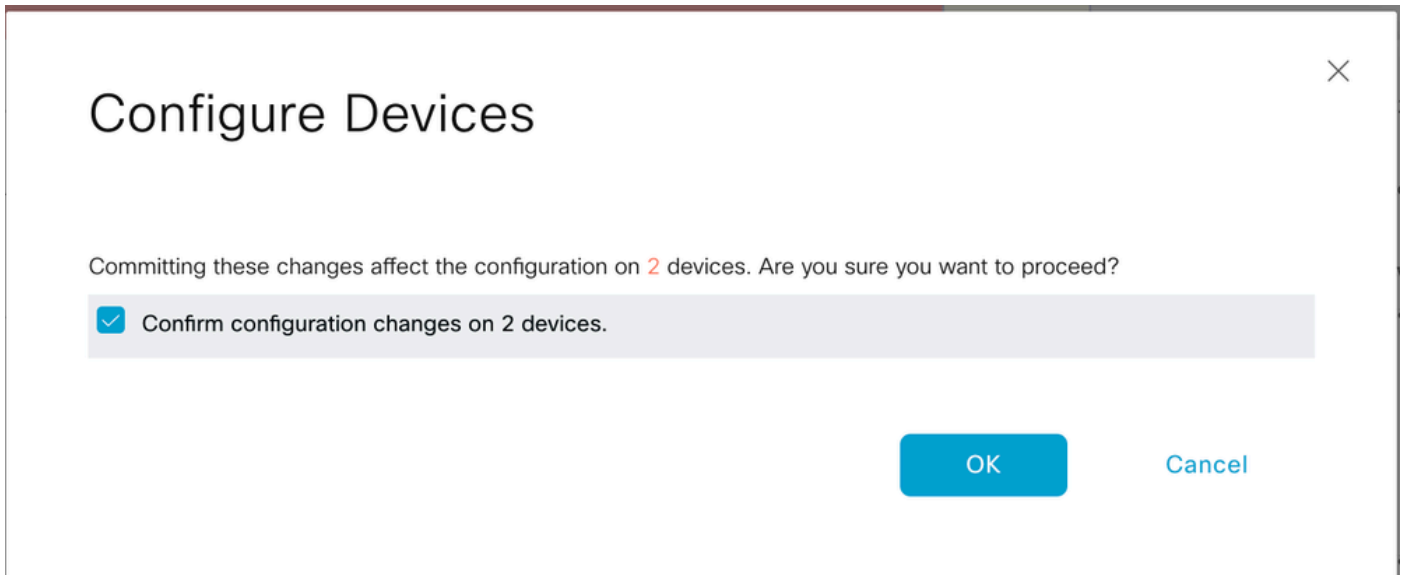
Device Template	Total	75	allow-service sshd	78	allow-service sshd
Site35_FeatureTemplate	1	76	no allow-service netconf	79	no allow-service netconf
		77	no allow-service ntp	80	no allow-service ntp
		78	no allow-service ospf	81	no allow-service ospf
		79	no allow-service stun	82	no allow-service stun
		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	!

Configure Device Rollback Timer

Back Configure Devices Cancel

Konfigurationsvorschau 2

6. Drücken Sie abschließend diese Konfiguration auf das Gerät:



Konfiguration bestätigen

Die nächste Ausgabe erfasst die aktuelle Konfiguration für VPN 0, sobald die Vorlage erfolgreich verschoben wurde:

Standort35_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#
```

Standort35_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#

```

Verifizierung

1. Die Vorlage wurde beiden Geräten erfolgreich zugeordnet:

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
Success	Done - Push Feature Template Con...	ISR1100-4GLTENA-FGL2347LJ1G	ISR 1100 4GLTE* (Viptela OS)	vEdge	10.10.10.19	35	10.10.10.1

Log details for the first device (ISR1100-4GLTEGB-FGL2347LHT6):

```

[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

```

Erfolg beim Push-Vorlagenzugriff

2. Die Steuerverbindung ist über das primäre WAN und die TLOC-Ext-Schnittstelle aktiv:

```
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#
```

Überprüfung der Kontrollverbindung 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

Überprüfung der Kontrollverbindung 2

Anwendungsfälle

Je nach lokalem Standortdesign kann die TLOC-Erweiterung auch mithilfe der L2- oder L3-TLOC-Erweiterung implementiert werden.

1. L2-TLOC-Erweiterung: Diese Erweiterungen befinden sich in derselben Broadcast-Domäne oder im gleichen Subnetz.
2. L3 TLOC-Erweiterung: Diese Erweiterungen sind durch ein L3-Gerät getrennt und können jedes Routing-Protokoll ausführen (wird nur auf Cisco IOSXE SD-WAN-Geräten unterstützt)



Hinweis: Siehe Abschnitt zu den TLOC-Erweiterungen im Kapitel "WAN Edge Deployment" des [Cisco SD-WAN-Designleitfadens](#).

Einschränkungen

- TLOC- und TLOC-Erweiterungsschnittstellen werden nur auf gerouteten L3-Schnittstellen unterstützt. L2-Switch-Ports/SVIs können nicht als WAN/Tunnel-Schnittstellen verwendet werden und können nur auf der Serviceseite verwendet werden.
- LTE wird auch nicht als TLOC-Erweiterungsschnittstelle zwischen WAN-Edge-Routern verwendet.
- L3 TLOC-Erweiterungen werden nur auf Cisco IOSXE SD-WAN-Routern und nicht auf vEdge-Routern unterstützt.
- Die TLOC-Erweiterung funktioniert nicht an Transportschnittstellen, die an Loopback-Tunnelschnittstellen gebunden sind.

Zugehörige Informationen

- [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.