Konfiguration eines SD-WAN-Edge-Routers für die Inline-Bereitstellung

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie der Cisco SD-WAN-Edge mit MPLS-Transport konfiguriert wird, um über den Inline-WAN-Edge des Rechenzentrums auf die Cisco SD-WAN-Controller im Internet zuzugreifen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

- Cisco Software-Defined Wide Area Network (SD-WAN)
- Routing

Verwendete Komponenten

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

- Cisco vManage, Version 20.6.5.2
- Cisco WAN Edge-Router Version 17.06.05

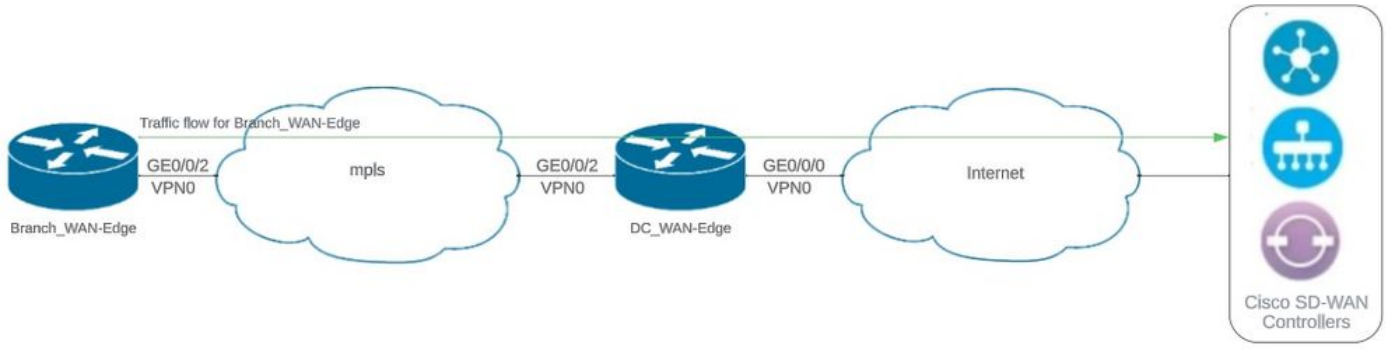
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen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

Hintergrundinformationen

In einer Inline-WAN-Edge-Bereitstellung im Rechenzentrum muss der vom MPLS eingehende Kontrolldatenverkehr die SD-WAN-Controller im Internet erreichen. Der Datenverkehr kann in VPN 0 zwischen MPLS und dem Internet geroutet werden.

In diesem Fall muss die Tunnelkonfiguration aus den physischen Schnittstellen MPLS und Internet entfernt und auf zwei separaten Loopback-Schnittstellen platziert werden.

Netzwerkdiagramm



Netzwerktopologie

Konfigurationen

Bei dieser Bereitstellung muss das Zweigstellen-WAN-Edge-Gerät über das WAN-Edge des Rechenzentrums auf die Controller zugreifen. In diesem Szenario wird dem VPN 0 am WAN-Edge des Rechenzentrums eine zusätzliche physische Schnittstelle hinzugefügt, und Tunnel werden von der physischen Schnittstelle zur Loopback-Schnittstelle verschoben.

Durch die Verschiebung des Tunnels von der physischen Schnittstelle zur Loopback-Schnittstelle kann der WAN-Edge-Router des Rechenzentrums als Transit für den Datenverkehr vom WAN-Edge des Rechenzentrums und vom WAN-Edge-Router der Außenstelle fungieren. Zwischen Loopback-IP-Adressen und Controllern muss eine Verbindung bestehen, um die Kontroll- und Datenebene zu bilden.

Diese Ausgabe erfasst die Konfiguration der WAN-Edge-Schnittstelle des RZ:

```
interface GigabitEthernet0/0/0
 ip address 10.201.186.175 255.255.255.224
 no shutdown
!
interface GigabitEthernet0/0/2
 description connection to Branch_WAN-Edge
 ip address 192.168.20.21 255.255.255.252
 no shutdown
!
interface Loopback1
 description wan_color_green
 ip address 192.168.20.2 255.255.255.255
```

```
 no shutdown
!
interface Loopback2
 description wan_color_custom2
 ip address 192.168.20.10 255.255.255.255
 no shutdown
!
```

Die nächste Ausgabe erfasst die Konfiguration des WAN-Edge-Tunnels im Rechenzentrum:

```
DC_WAN-Edge#sh sdwan running-config sdwan
sdwan
 interface Loopback1
  tunnel-interface
   encapsulation ipsec weight 1
   no border
   color green
   no last-resort-circuit
   no low-bandwidth-link
   max-control-connections 1
   no vbond-as-stun-server
   vmanage-connection-preference 5
   port-hop
   carrier                       default
   nat-refresh-interval          5
   hello-interval                1000
   hello-tolerance               12
   no allow-service all
   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 allow-service snmp
   no allow-service bfd
  exit
 exit
 interface Loopback2
  tunnel-interface
   encapsulation ipsec weight 1
   no border
   color custom2 restrict
   no last-resort-circuit
   no low-bandwidth-link
   max-control-connections 1
   no vbond-as-stun-server
   vmanage-connection-preference 5
   port-hop
   carrier default
   nat-refresh-interval 5
   hello-interval 1000
   hello-tolerance 12
   no allow-service all
```

```
   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 allow-service snmp
   no allow-service bfd
  exit
 exit
!
```

Die nächste Ausgabe erfasst die Konfiguration des Branch_WAN-Edge-Tunnels:

```
Branch_WAN-Edge#sh sdwan run sdwan
sdwan
 interface GigabitEthernet0/0/2
  tunnel-interface
   encapsulation ipsec weight 1
   no border
   color custom2
   no last-resort-circuit
   no low-bandwidth-link
   no vbond-as-stun-server
   vmanage-connection-preference 5
   port-hop
   carrier                       default
   nat-refresh-interval          5
   hello-interval                1000
   hello-tolerance               12
   no allow-service all
   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 http
   no allow-service snmp
   no allow-service bfd
  exit
 exit
!
```

Verifizierung

Die nächste Ausgabe erfasst die Konnektivität der Kontrollebene für DC_WAN-Edge.

```
DC_WAN-Edge#sh sdwan control connections
PEER PEER CONTROLLER
PEER PEER PEER SITE DOMAIN PEER PRIV PEER PUB GROUP
TYPE PROT SYSTEM IP ID ID PRIVATE IP PORT PUBLIC IP PORT ORGANIZATION LOCAL COLOR PROXY STATE UPTIME ID
------------------------------------------------------------------------------------------------------
vsmart dtls 10.10.10.2 1 1 10.201.186.172 12346 10.201.186.172 12346 rch_sdwan_lab custom2 No up 0:00:0
vsmart dtls 10.10.10.2 1 1 10.201.186.172 12346 10.201.186.172 12346 rch_sdwan_lab green No up 0:00:00:
vmanage dtls 10.10.10.1 1 0 10.201.186.171 12746 10.201.186.171 12746 rch_sdwan_lab green No up 0:00:00
```

Die nächste Ausgabe erfasst die Konnektivität der Kontrollebene für Branch_WAN-Edge.

```
Branch_WAN-Edge#show sdwan control connections
PEER PEER CONTROLLER
PEER PEER PEER SITE DOMAIN PEER PRIV PEER PUB GROUP
TYPE PROT SYSTEM IP ID ID PRIVATE IP PORT PUBLIC IP PORT LOCAL COLOR PROXY STATE UPTIME ID
------------------------------------------------------------------------------------------------------
vsmart dtls 10.10.10.2 1 1 10.201.186.172 12346 10.201.186.172 12346 custom2 No up 0:00:00:20 0
vmanage dtls 10.10.10.1 1 0 10.201.186.171 12346 10.201.186.171 12346 custom2 No up 0:00:00:22 0
```

Die nächste Ausgabe erfasst die Datenebenenverbindung für DC_WAN-Edge. Die lokale Farbe Grün bildet eine BFD-Sitzung mit Remote-Edge-Geräten.

```
DC_WAN-Edge#sh sdwan bfd sessions
SOURCE TLOC REMOTE TLOC DST PUBLIC DST PUBLIC DETECT TX
SYSTEM IP SITE ID STATE COLOR COLOR SOURCE IP IP PORT ENCAP MULTIPLIER INTERVAL(msec UPTIME TRANSITIONS
------------------------------------------------------------------------------------------------------
10.10.10.60 60 up green biz-internet 192.168.20.2 10.201.186.167 12346 ipsec 7 1000 0:00:06:37 6
10.10.10.20 20 up green biz-internet 192.168.20.2 10.201.186.180 12346 ipsec 7 1000 0:00:06:37 6
10.10.10.5 5 up green default 192.168.20.2 10.201.186.181 12346 ipsec 7 1000 0:00:06:37 6
10.10.10.10 10 up green gold 192.168.20.2 10.201.186.182 12346 ipsec 7 1000 0:00:06:37 6
```

Die nächste Ausgabe erfasst die Verbindungen der Datenebene für Branch_WAN-Edge. Die lokale Farbe custom2 bildet eine BFD-Sitzung mit Remote-Edge-Geräten.

```
Branch_WAN-Edge#sh sdwan bfd sessions
SOURCE TLOC REMOTE TLOC DST PUBLIC DST PUBLIC DETECT TX
SYSTEM IP SITE ID STATE COLOR COLOR SOURCE IP IP PORT ENCAP MULTIPLIER INTERVAL(msec) UPTIME TRANSITION
------------------------------------------------------------------------------------------------------
10.10.10.5 5 up custom2 default 192.168.20.22 10.201.186.181 12346 ipsec 7 1000 0:00:07:37 2
10.10.10.10 10 up custom2 gold 192.168.20.22 10.201.186.182 12346 ipsec 7 1000 0:00:07:37 2
10.10.10.20 20 up custom2 biz-internet 192.168.20.22 10.201.186.180 12346 ipsec 7 1000 0:00:07:37 2
10.10.10.60 60 up custom2 biz-internet 192.168.20.22 10.201.186.167 12346 ipsec 7 1000 0:00:07:37 2
```

Zugehörige Informationen

- Cisco SD-WAN-Designleitfaden

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.