为SDWAN实施直接互联网接入

目录

简介

先决条件

- 要求
- 使用的组件

网络图

配置

- 在传输接口上启用NAT
- 来自服务VPN的直接流量
- 集中数据策略

确认

- 无DIA
- 使用DIA
- 集中数据策略

简介

本文档介绍如何实施Cisco SD-WAN DIA。它是指互联网流量直接从路由器中断时的配置。

先决条件

要求

Cisco 建议您了解以下主题：

- 网络地址转换 (NAT)
- 思科软件定义的广域网(SD-WAN)

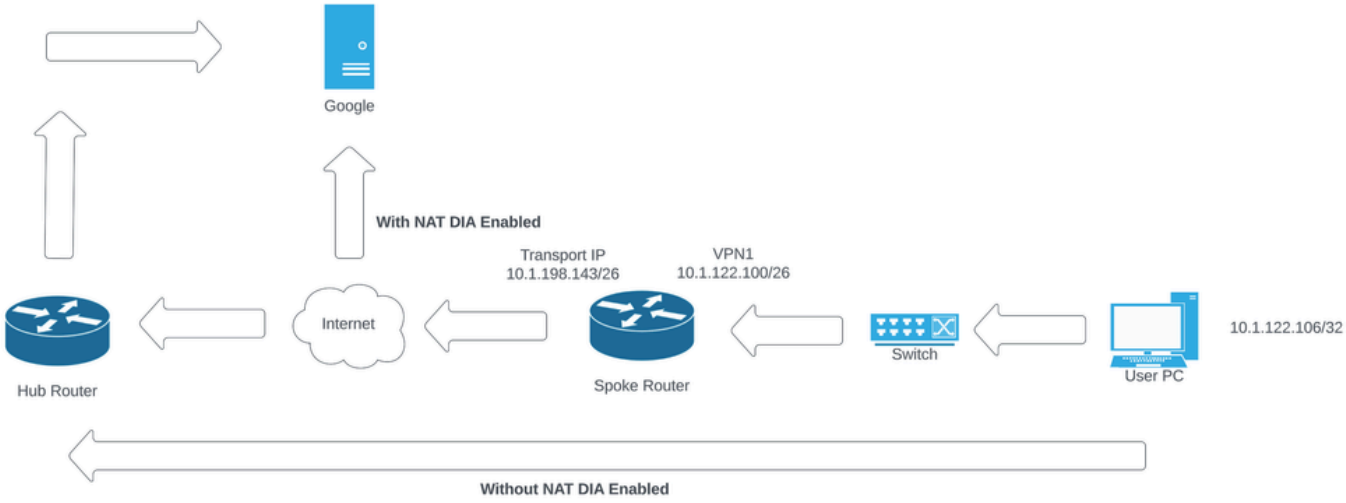
使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科vManage版本20.6.3
- 思科广域网边缘路由器17.4.2

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

网络图



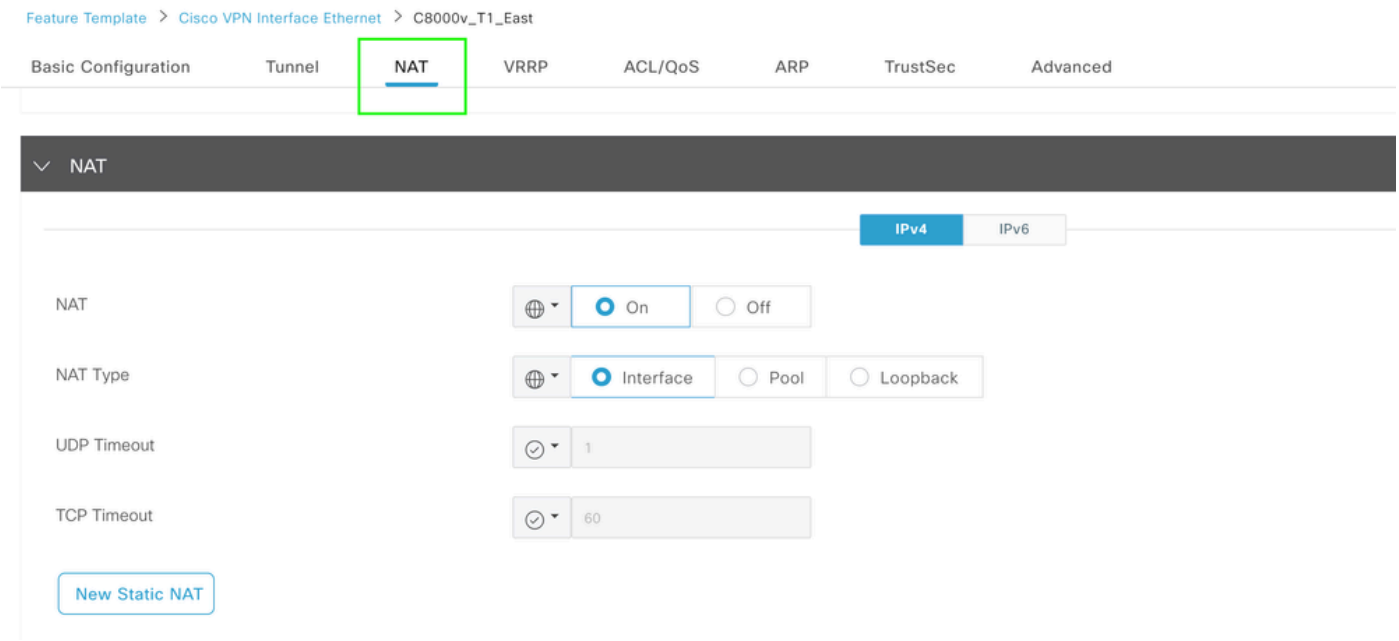
网络拓扑

配置

思科SD-WAN路由器上的DIA分两个步骤启用：

- 在传输接口上启用NAT。
- 通过静态路由或集中数据策略从服务VPN定向流量。

在传输接口上启用NAT



VPN接口NAT模板

配置在NAT后（启用后）显示如下：

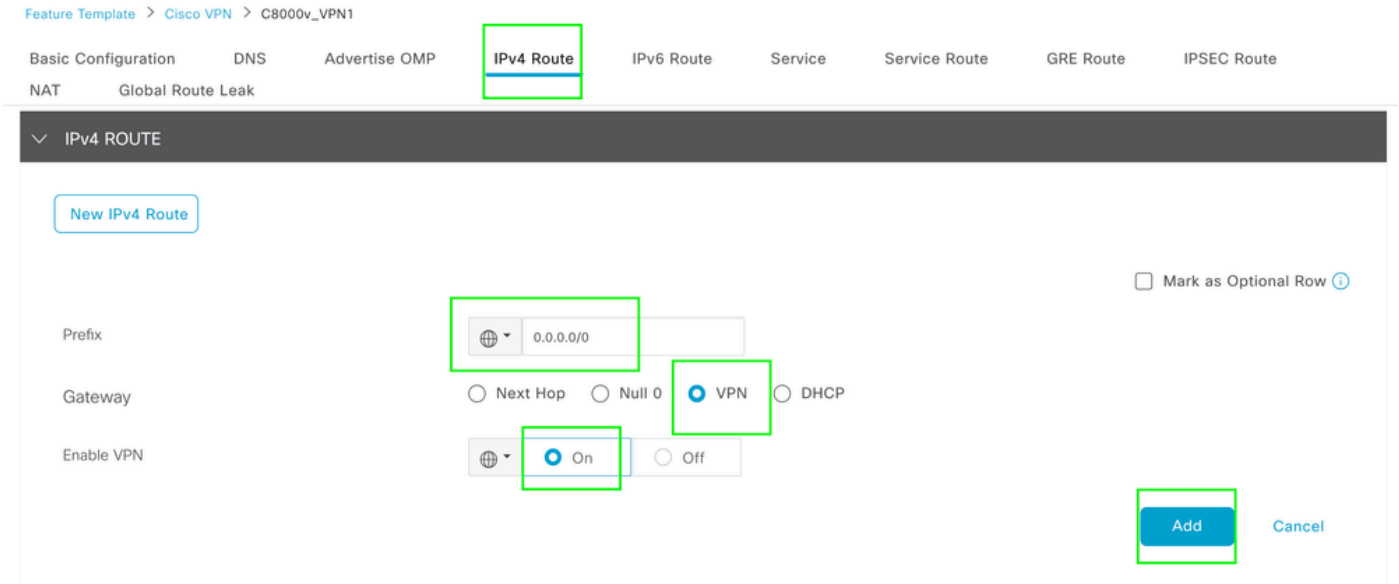
```
ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet2 overload
ip nat translation tcp-timeout 3600
ip nat translation udp-timeout 60

interface GigabitEthernet2
ip nat outside
```

来自服务VPN的直接流量

这可以通过两种方式实现：

- 静态NAT路由：必须在服务VPN 1功能模板下创建静态NAT路由。



VPN 1 IPV4路由模板

此行作为配置的一部分推送：

```
ip nat route vrf 1 0.0.0.0 0.0.0.0 global
```

集中数据策略

1.创建数据前缀列表，以便特定用户可以通过DIA访问Internet。



集中策略自定义数据前缀列表

2.创建VPN列表，以便特定VPN用户可以发起流量。



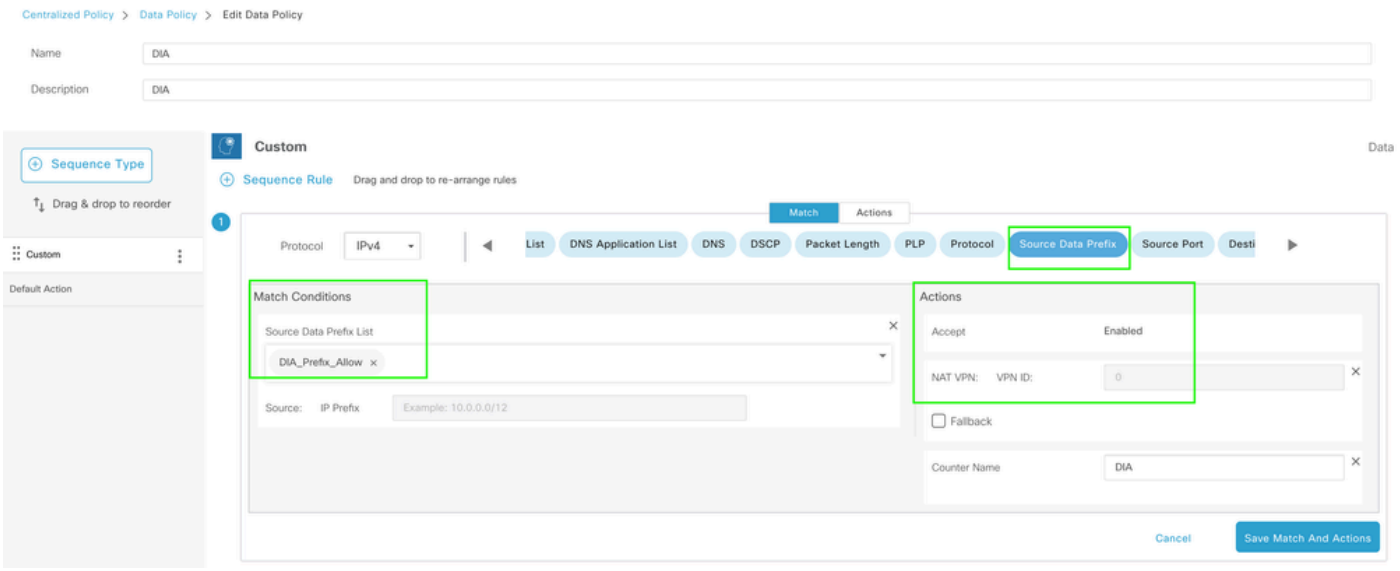
集中策略自定义VPN列表

3.创建站点列表；这允许将策略应用于特定站点。



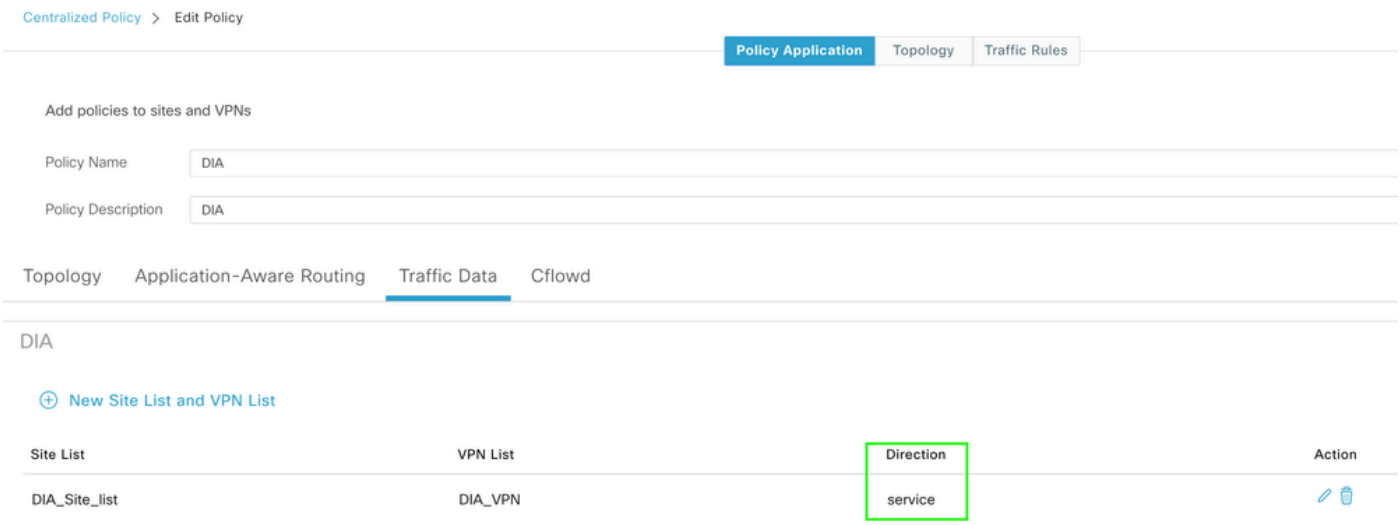
集中策略自定义站点列表

4.创建自定义数据策略以匹配源数据前缀。然后，将操作设置为使用NAT VPN 0，这样允许它遍历到DIA。



集中数据策略

5.此政策的方向必须是服务端。



流量数据规则

6.这是集中数据策略的预览：

```
viptela-policy:policy
 data-policy _DIA_VPN_DIA
  vpn-list DIA_VPN
    sequence 1
     match
      source-data-prefix-list DIA_Prefix_Allow
     !
```

```
     action accept
      nat use-vpn 0
      count DIA_1164863292
     !
    !
  default-action accept
 !
 lists
  data-prefix-list DIA_Prefix_Allow
   ip-prefix 10.1.122.106/32
  !
  site-list DIA_Site_list
   site-id 100004
  !
  vpn-list DIA_VPN
   vpn 1
  !
 !
!
apply-policy
 site-list DIA_Site_list
  data-policy _DIA_VPN_DIA from-service
 !
!
```

确认

无DIA

下一个输出捕获在服务端未启用NAT DIA时：

```
cEdge_Site1_East_01#show ip route vrf 1 nat-route

Routing Table: 1
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set
```

```
cEdge_Site1_East_01#
```

默认情况下，VPN 1上的用户无法访问Internet:

```
C:\Users\Administrator>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 10.1.122.100: Destination host unreachable.
Reply from 10.1.122.100: Destination host unreachable.
Reply from 10.1.122.100: Destination host unreachable.
Reply from 10.1.122.100: Destination host unreachable.

Ping statistics for 8.8.8.8:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\Administrator>
```

使用DIA

静态NAT路由:下一个输出捕获在服务端启用的NAT DIA:

```
cEdge_Site1_East_01#show ip route vrf 1 nat-route

Routing Table: 1
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

n*Nd  0.0.0.0/0 [6/0], 01:41:46, Null0

cEdge_Site1_East_01#
```

VPN 1中的用户现在可以访问互联网：

```
C:\Users\Administrator>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=1ms TTL=52
Reply from 8.8.8.8: bytes=32 time=1ms TTL=52
Reply from 8.8.8.8: bytes=32 time=1ms TTL=52
Reply from 8.8.8.8: bytes=32 time=1ms TTL=52

Ping statistics for 8.8.8.8:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\Administrator>
```

后续输出捕获NAT转换：

```
cEdge_Site1_East_01#sh ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
icmp 10.1.198.143:1        10.1.122.106:1        8.8.8.8:1             8.8.8.8:1

Total number of translations: 1
```

下一命令捕获数据包必须采用的路径：

```
cEdge_Site1_East_01#show sdwan policy service-path vpn 1 interface GigabitEthernet 4 source-ip 10.1.122
Next Hop: Remote
  Remote IP: 10.1.198.129, Interface GigabitEthernet2 Index: 8
```

集中数据策略

将集中数据策略推送到vSmart后，可以在广域网边缘设备上使用show sdwan policy from-vsmart data-policy命令验证设备已收到哪些策略：

```
cEdge_Site1_East_01#show sdwan policy from-vsmart data-policy
from-vsmart data-policy _DIA_VPN_DIA
 direction from-service
 vpn-list DIA_VPN
  sequence 1
   match
    source-data-prefix-list DIA_Prefix_Allow
   action accept
    count DIA_1164863292
    nat use-vpn 0
    no nat fallback
  default-action accept
```

```
cEdge_Site1_East_01#
```

VPN 1中的用户现在可以访问互联网：

```
C:\Users\Administrator>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=4ms TTL=52
Reply from 8.8.8.8: bytes=32 time=1ms TTL=52
Reply from 8.8.8.8: bytes=32 time=1ms TTL=52
Reply from 8.8.8.8: bytes=32 time=1ms TTL=52

Ping statistics for 8.8.8.8:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 4ms, Average = 1ms

C:\Users\Administrator>
```

下一命令捕获数据包必须采用的路径：

```
cEdge_Site1_East_01#show sdwan policy service-path vpn 1 interface GigabitEthernet 4 source-ip 10.1.122
Next Hop: Remote
  Remote IP: 10.1.198.129, Interface GigabitEthernet2 Index: 8
```

后续输出捕获NAT转换：

```
cEdge_Site1_East_01#sh ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
icmp 10.1.198.143:1        10.1.122.106:1        8.8.8.8:1             8.8.8.8:1

Total number of translations: 1
```

此输出捕获计数器增量：

```
cEdge_Site1_East_01#show sdwan policy data-policy-filter
data-policy-filter _DIA_VPN_DIA
 data-policy-vpnlist DIA_VPN
  data-policy-counter DIA_1164863292
   packets 4
   bytes   296
```

```
  data-policy-counter default_action_count
   packets 0
   bytes   0

cEdge_Site1_East_01#
```

此输出捕获由于源IP不属于数据前缀列表而被黑洞的流量：

```
cEdge_Site1_East_01#show sdwan policy service-path vpn 1 interface GigabitEthernet 4 source-ip 10.1.122
Next Hop: Blackhole

cEdge_Site1_East_01#
```

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。