SD-WAN용 DIA(Direct Internet Access) 구현

목차

<u>소개</u> <u>사전 요구 사항</u> <u>요구 사항</u> <u>사용되는 구성 요소</u> <u>네트워크 다이어그램</u> <u>설정</u> <u>전송 인터페이스에서 NAT 활성화</u> <u>서비스 VPN에서 직접 트래픽</u> <u>확인</u> <u>DIA 없음</u> <u>DIA 사용</u>

소개

이 문서에서는 Cisco SD-WAN DIA를 구현하는 방법에 대해 설명합니다. 인터넷 트래픽이 브랜치 라우터에서 직접 발생하는 경우를 컨피그레이션이라고 합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco SD-WAN(Software-defined Wide Area Network)
- NAT(Network Address Translation)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco vManage 버전 20.6.3
- Cisco WAN Edge Router 17.4.2

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

네트워크 다이어그램

\sim	Google	
	With NAT DIA Enabled	
	Transport IP VPN1 10.1.198.143/26 10.1.122.100/26	
		10.1.122.106/32
Hub Router	Spoke Router USer PC	
$\langle -$		
0	Without NAT DIA Enabled	

네트워크 토폴로지

설정

Cisco SD-WAN 라우터의 DIA는 두 단계로 활성화됩니다.

1. 전송 인터페이스에서 NAT를 활성화합니다.

2. 고정 경로 또는 중앙 집중식 데이터 정책을 사용하여 서비스 VPN에서 직접 트래픽을 전송합니다

전송 인터페이스에서 NAT 활성화

eature Template > Cisco VPN I	Interface Etherr	net > C8000v	_T1_East					
asic Configuration	Tunnel	NAT	VRRP	ACL/QoS	ARP	TrustSec	Advanced	
∕ NAT								
						IPv4	IPv6	
NAT			•	O On (Off			
NATTING						0		
NAT Type			•	Interface	O Pool	O Loopback		
UDP Timeout			Ø •					
TOD Timeout								
TOP TIMEOUL								
New Static NAT								

VPN 인터페이스 NAT 템플릿

이는 컨피그레이션에서 POST NAT가 활성화된 것처럼 보이는 방식입니다.

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

서비스 VPN에서 직접 트래픽

이는 다음 두 가지 방법으로 달성할 수 있습니다.

1. 고정 NAT 경로: 서비스 VPN 1 기능 템플릿 아래에 고정 NAT 경로를 생성해야 합니다.

Feature Template > Cisco VPN > C8000v_VPN1					
Basic Configuration DNS Advertise C	IPv4 Route IP	Pv6 Route Service	Service Route	GRE Route	IPSEC Route
NAT Global Route Leak					
✓ IPv4 ROUTE					
New IPv4 Route					
				□ N	/lark as Optional Row 🛈
Prefix	• • 0.0.0.0/0				
Gateway	O Next Hop O Nul				
Enable VPN	••• • • • • • • • • • • • • • • • • •	Off			
					Add Cancel

VPN 1 IPV4 경로 템플릿

이 라인은 컨피그레이션의 일부로 푸시됩니다.

ip nat route vrf 1 0.0.0.0 0.0.0.0 global

2. 중앙 집중식 데이터 정책

특정 사용자가 DIA를 통해 인터넷에 액세스할 수 있도록 데이터 접두사 목록을 만듭니다.

Centralized Policy > Define Lists

ິ່ | ິ່ງ Custom Options ∨

Select a list type on the left and start creating your groups of interest

Application	New Data Prefix	List					
Color							
Community	Name	Entries	Internet Protocol	Reference Count	Updated By	Last Updated	Action
Data Prefix	DIA_Prefix_Allow	10.1.122.106/32	IPv4	1	admin	18 Jul 2023 9:31:26 AM CDT	000
Policer							
Prefix							
Site							
App Probe Class							
SLA Class							
TLOC							
VPN							

중앙 정책 사용자 지정 데이터 접두사 목록

특정 VPN 사용자가 트래픽을 시작할 수 있도록 VPN 목록을 생성합니다.

Centralized Policy > Define Lists						ໃ¦່ໃ Custom Options ∽		
Select a list type on the left and start creating your groups of interest								
Application	New VPN List							
Color								
Community	Name	Entries	Reference Count	Updated By	Last Updated	Action		
Data Prefix	DIA_VPN	1	1	admin	18 Jul 2023 9:56:21 AM CDT	000		
Policer								
Prefix								
Site								
App Probe Class								
SLA Class								
TLOC								
VPN								

중앙 집중식 정책 맞춤형 VPN 목록

특정 사이트에 정책을 적용할 수 있도록 사이트 목록을 생성합니다.

Centralized Policy > Define Lists						Image: State of the state o		
Select a list type on the left and start creating your groups of interest								
Application Color	New Site List							
Community	Name	Entries	Reference Count	Updated By	Last Updated	Action		
Data Prefix	DIA_Site_list	100004	1	admin	18 Jul 2023 10:03:59 AM CDT	000		
Policer								
Prefix								
Site								
App Probe Class								
SLA Class								
TLOC								
VPN								

중앙 정책 사용자 지정 사이트 목록

소스 데이터 접두사를 일치시키기 위해 사용자 지정 데이터 정책을 생성하고 DIA를 통과할 수 있도 록 NAT VPN 0을 사용하도록 작업을 설정합니다.

Centralized Policy >	Data Policy >	Edit Data Policy					
Name	DIA						
Description	DIA						
Sequence Type Type	a	Custom Sequence Rule Drag and drop to re-arrange rules Match Action	ins -				Dat
Custom	:	Protocol IPv4 • List DNS Application List DNS DSCP Packet Length	PI	LP Protocol Source	e Data Prefix Source Port	Desti 🕨	
Default Action		Match Conditions		Actions			
		Source Data Prefix List	×	Accept	Enabled		
		DIA_Prefix_Allow ×	*	NAT VPN: VPN ID:	0		×
		Source: IP Prefix Example: 10.0.0.0/12		Fallback			
				Counter Name	DIA		×
					Cancel	Save Match And	Actions

중앙 집중식 데이터 정책

이 정책의 방향은 서비스 쪽이어야 합니다.

			lit Policy	Centralized Policy > E		
Traffic Rules	cation Topology Traffic Rules	Policy Application				
			and VPNs	Add policies to sites		
			DIA	Policy Name		
			DIA	Policy Description		
Topology Application-Aware Routing Traffic Data Cflowd						
				DIA		
			nd VPN List	① New Site List a		
Action	Direction		VPN List	Site List		
/ Ô	service		DIA_VPN	DIA_Site_list		
Action	Direction service	Cflowd	DIA ation-Aware Routing Traffic Data nd VPN List VPN List DIA_VPN	Policy Description Topology Applic DIA		

트래픽 데이터 규칙

중앙 집중식 데이터 정책의 미리 보기입니다.

```
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
 I.
 lists
  data-prefix-list DIA_Prefix_Allow
   ip-prefix 10.1.122.106/32
  L
  site-list DIA_Site_list
  site-id 100004
  !
  vpn-list DIA_VPN
  vpn 1
  !
 Т
ï
apply-policy
site-list DIA_Site_list
  data-policy _DIA_VPN_DIA from-service
 !
!
```

확인

DIA 없음

다음 출력은 서비스 측에서 NAT DIA가 활성화되지 않은 경우 캡처합니다.

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, 1 - 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#

기본적으로 VPN 1의 사용자는 인터넷에 액세스할 수 없습니다.

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),

cEdge_Site1_East_01#show ip route vrf 1 nat-route

C:\Users\Administrator>

DIA 사용

1. 고정 NAT 경로: 다음 출력은 서비스 측에서 활성화된 NAT DIA를 캡처합니다.

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, 1 - 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#

이제 VPN 1의 사용자가 인터넷에 연결할 수 있습니다.

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>

후속 출력에서는 NAT 변환을 캡처합니다.

cEdge		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

다음 명령은 패킷이 취해야 하는 경로를 캡처합니다.

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

2. 중앙 집중식 데이터 정책

중앙 데이터 정책이 vSmart로 푸시되면 show sdwan policy from-vsmart data-policy 디바이스가 어떤 정책을 수 신했는지 확인하기 위해 WAN 에지 디바이스에서 명령을 사용할 수 있습니다.

```
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#

이제 VPN 1의 사용자가 인터넷에 연결할 수 있습니다.

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>

다음 명령은 패킷이 취해야 하는 경로를 캡처합니다.

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

후속 출력에서는 NAT 변환을 캡처합니다.

cEdge	e_Site1_East_01#sh i	p 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

이 출력은 카운터 증분을 캡처합니다.

```
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#

이 출력은 소스 IP가 데이터 접두사 목록에 속하지 않기 때문에 블랙홀링된 트래픽을 캡처합니다.

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#

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번 역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.