NAT를 사용하는 경우 vEdge에서 IPSec 터널을 설정할 수 없는 이유는 무엇입니까?

목차

소개 <u>배경 정보</u> 문제 <u>작업 시나리오</u> 실패 시나리오 솔루션 <u>NAT 포트 전달</u> 명시적 ACL 기타 고려 사항 결론

소개

이 문서에서는 vEdge 라우터가 데이터 플레인 터널에 IPSec 캡슐화를 사용하고 있고 한 디바이스 가 대칭 NAT(RFC3489) 또는 RFC4787(Address Dependent Mapping)를 수행하는 NAT(Network Address Translation) 디바이스 뒤에 있을 때, 다른 라우터가 DIA(Direct Internet Access) 또는 전송 측 인터페이스에 구성된 일부 NAT 유형에 대해 설명합니다.

배경 정보

참고:이 문서는 vEdge 라우터에만 적용되며 vEdge 소프트웨어 18.4.1 및 19.1.0에서 보이는 동작을 기반으로 작성되었습니다. 최신 릴리스의 동작은 다를 수 있습니다.문의 사항이 있을 경우 설명서를 참조하거나 Cisco TAC(Technical Assistance Center)에 문의하십시오.

이 데모에서는 SD-WAN TAC 실습에서 문제가 다시 발생했습니다.디바이스 설정은 다음 표에 요약 되어 있습니다.

호스트 사이 이름 트 ID 시스템 IP 전용 ip 공용 ip

vodao1	າວາ	10.10.10.	192.168.10	198.51.100
veuger	232	232	.232	.232
vodao2		10.10.10.	192.168.9.	192.168.9.
veugez	233	233	233	233
vomort	1	10.10.10.	192.168.0.	192.168.0.
vsman	I	228	228	228
vbond	1	10.10.10.	192.168.0.	192.168.0.
vuona	I	231	231	231

전송 측 컨피그레이션은 두 디바이스 모두에서 매우 일반적입니다.다음은 vEdge1의 컨피그레이션 입니다.

```
vpn 0
 interface ge0/0
  ip address 192.168.10.232/24
  !
  tunnel-interface
   encapsulation ipsec
   color biz-internet
  no allow-service bgp
   no 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
  1
 no shutdown
 !
 ip route 0.0.0.0/0 192.168.10.11
!
vEdge2:
```

```
interface ge0/1
  ip address 192.168.9.233/24
  tunnel-interface
   encapsulation ipsec
   color biz-internet
  no allow-service bgp
  no 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
  Ţ
 no shutdown
 Ţ
```

```
ip route 0.0.0.0/0 192.168.9.1
```

이 문서에서 문제를 시연하기 위해 ASAv(Virtual Adaptive Security Appliance) 방화벽은 두 vEdge 라우터 사이에 있습니다.ASAv는 다음 규칙에 따라 주소 변환을 수행합니다.

- vEdge1의 트래픽이 컨트롤러에 대한 것이면 소스 포트 12346-12426이 52346-52426으로 변환 됩니다.
- vEdge1의 트래픽이 다른 사이트로의 데이터 플레인 연결을 위해 사용되는 경우 소스 포트 12346-12426은 42346-42426으로 변환됩니다.
- vEdge1의 다른 모든 트래픽도 동일한 공용 주소(198.51.100.232)에 매핑됩니다.
- 참조용 ASAv NAT 컨피그레이션입니다.

subnet 192.168.0.0 255.255.255.0 object network VE1_NAT host 198.51.100.232 object service CONTROL service udp source range 12346 12445 destination range 12346 12445 object service CC_NAT_CONTROLLERS service udp source range 52346 52445 destination range 12346 12445 object service CC_NAT_OTHER service udp source range 42346 42445 destination range 12346 12445 object network ALL subnet 0.0.0.0 0.0.0.0 nat (ve1-iface, ve2-iface) source static VE1 VE1_NAT destination static CONTROLLERS CONTROLLERS service CONTROL CC_NAT_CONTROLLERS nat (vel-iface, ve2-iface) source static VE1 VE1_NAT destination static ALL ALL service CONTROL CC_NAT_OTHER nat (vel-iface, ve2-iface) source dynamic VE1 VE1_NAT

작업 시나리오

정상 상태에서는 데이터 평면 터널이 설정되고 BFD(Bidirectional Forwarding Detection)가 up 상태 **에 있음을** 확인할 수 있습니다.

컨트롤러와의 제어 연결을 설정하기 위해 vEdge1 디바이스(52366)에서 어떤 공용 포트를 사용하 는지 확인하십시오.

vEdge1# show control local-properties wan-interface-list

NAT TYPE: E -- indicates End-point independent mapping A -- indicates Address-port dependent mapping N -- indicates Not learned Note: Requires minimum two vbonds to learn the NAT type

		PU	PUBLIC		PUBLIC PRIVATE			PRIVATE			
PRIVATE	2		MA		MAX RESTRICT/		LAST		SPI TIME	NAT	VM
INTERFA	ACE	IP	v4	Р	ORT	IPv4		IPv6			
PORT	VS/VM	COLOR	STATE	CNTRL	CONT	ROL/	LR/LB	CONNECTION	REMAINING	TYPE	CON
STUN						PRF					
~~~~ (0		10	0 51 100	000 E	2266	100 160	10 222				
geu/u		19	0.01.100.	232 3	2300	192.100	.10.232	::			
12366	2/1	biz-internet	up	2	no	/yes/no	No/No	0:00:00:28	0:11:59:17	N	5

#### vEdge2에서 NAT가 사용되지 않으므로 개인 주소와 포트는 동일합니다.

vEdge2# show control local-properties wan-interface-list

NAT TYPE: E -- indicates End-point independent mapping A -- indicates Address-port dependent mapping N -- indicates Not learned Note: Requires minimum two vbonds to learn the NAT type

	PUBLIC	PUBLIC PRIVATE	PRIVATE		
PRIVATE		MAX RESTRICT/	LAST	SPI TIME	NAT VM
INTERFACE	IPv4	PORT IPv4	IPv6		

PORT	VS/VM	COLOR	STATE CNTRI	CONTROL/	LR/LB	CONNECTION	REMAINING	TYPE	CON
STUN				PRF					
ge0/1		192.1	68.9.233 1	2366 192.168	.9.233	::			
12366	2/1	biz-internet	up 2	no/yes/no	No/No	0:00:00:48	0:11:58:53	Ν	5

## vEdge1의 show tunnel 통계에서 tx/rx 카운터가 증가하고 있음을 확인할 수 있습니다.

vEdge1# show tunnel statistics dest-ip 192.168.9.233

TCP								
TUNNEL				SOURCE	DEST			
TUNNEL					MSS			
PROTOCOI	SOURCE	IP	DEST IP	PORT	PORT	SYSTEM IP	LOCAL COLOR	REMOTE COLOR
MTU	tx-pkts	tx-octets	s rx-pkts	rx-octets	ADJUST			
ipsec	192.16	8.10.232	192.168.9.	233 12366	12366	10.10.10.233	biz-internet	biz-internet
1441	223	81163	179	40201	1202			

#### vEdge2의 동일한 출력에서 rx/rx 패킷 카운터가 증가함을 확인할 수 있습니다.대상 포트(42366)가 제어 연결을 설정하는 데 사용되는 포트와 다릅니다(52366).

vEdge2# show tunnel statistics dest-ip 198.51.100.232

TCP SOURCE DEST TUNNEL. TUNNEL MSS SYSTEM IP LOCAL COLOR REMOTE COLOR PORT PROTOCOL SOURCE IP DEST IP PORT MTU tx-pkts tx-octets rx-pkts rx-octets ADJUST _____ _____ ipsec 192.168.9.233 198.51.100.232 12366 42366 10.10.10.232 biz-internet biz-internet 1441 296 88669 261 44638 1201

#### 그러나 BFD 세션은 두 디바이스 모두에서 여전히 가동 중입니다.

vEdge1# show bfd sessions site-id 233 | tab

 SRC
 DST
 SITE

 DETECT
 TX

 SRC IP
 DST IP
 PROTO
 PORT
 PORT
 SYSTEM IP
 ID
 LOCAL COLOR
 COLOR

 STATE
 MULTIPLIER
 INTERVAL
 UPTIME
 TRANSITIONS
 TRANSITIONS
 TRANSITIONS

 192.168.10.232
 192.168.9.233
 ipsec
 12366
 12366
 10.10.10.233
 233
 biz-internet
 biz-internet

 internet
 up
 7
 1000
 0:00:02:42
 0
 0

vEdge2# show bfd sessions site-id 232 | tab

컨트롤 및 데이터 플레인 연결에 사용되는 포트가 다르더라도 문제가 발생하지 않으며 연결이 제자 리에 있습니다.

## 실패 시나리오

사용자가 vEdge2 라우터에서 DIA(Direct Internet Access)를 활성화하려고 합니다.이를 위해 이 컨 피그레이션은 vEdge2에 적용되었습니다.

vpn 0
interface ge0/1
nat
respond-to-ping
!
!
vpn 1
ip route 0.0.0.0/0 vpn 0
!

그리고 BFD 세션이 예기치 않게 중단되었으며 다운된 상태를 유지합니다.터널 통계를 지운 후 show tunnel statistics 출력에서 RX 카운터가 증가하지 않음을 확인할 수 있습니다.

vEdge2# show tunnel statistics dest-ip 198.51.100.232

TCP TUNNEL TUNNEL PROTOCOL	SOURCE	IP	DEST IF	2	SOURCE PORT	DEST MSS PORT	SYSTEM	IP	LOCAL COLOR	REMOTE	COLOR
MTU	tx-pkts	tx-octet	ts rx-p	okts ra	-octets	ADJUST					
 		· · · · · · · · · · · · · · · · · · ·	100 51	100 222	10246	 	10 10	10 222	hig internet	bis in	
1//2	192.100 282	18222	190.51.	. 100.232 0	12340	1368	10.10.	10.232	prz-incernet	012-110	Lerner
1442	202	40222	0	0		1000					
vEdge2#	show bfd	sessions	s site-i	ld 232							
				ç	OURCE TL	C	REMOTE 1	FLOC			
DST PUBL	IC			DST PUE	BLIC	DETE	ECT	TX			
SYSTEM I	Р	SITE ID	STATE	C	OLOR		COLOR		SOURCE IP		
IP				PORT	ENC	AP MULI	TIPLIER	INTERV	AL(msec) UPTIM	ΙE	
TRANSITI	ONS										
10.10.10 198.51.1	.232 00.232	232	down	k 52366	oiz-intern ipso	net ec 7	biz-inte	ernet 1000	192.168.9.2 NA	33	0

TCP								
TUNNEL				SOURC	CE DEST			
TUNNEL					MSS			
PROTOCOI	SOURCE	IP I	DEST IP	PORT	PORT	SYSTEM IP	LOCAL COLOR	REMOTE COLOR
MTU	tx-pkts	tx-octets	s rx-pkts	rx-octets	adjust			
ipsec	192.168	3.9.233 1	98.51.100	.232 12346	5 52366	10.10.10.232	biz-internet	biz-internet
1442	285	48735	0	0	1368			

처음에는 고객이 터널 MTU와 관련된 문제를 의심했습니다.위의 출력을 "작업 시나리오" 섹션의 출 력과 비교할 경우 작업 시나리오에서 터널 MTU는 1441이고 실패한 시나리오의 경우 1442입니다. 설명서를 기반으로 터널 MTU는 1442(터널 오버헤드의 경우 1500 기본 인터페이스 MTU - 58바이 트)여야 하지만 BTU가 up이면 터널 MTU는 1바이트로 줄어듭니다.참조를 위해 show tunnel statistics의 출력과 show tunnel statistics bfd가 down 상태에 있는 경우 아래에 제공된 출력

vEdge1# show tunnel statistics dest-ip 192.168.9.233 ; show tunnel statistics bfd dest-ip 192.168.9.233

TCP TUNNEL TUNNEL PROTOCOI MTU	SOURCE	IP tx-octet	DEST IP s rx-pkts	rx-	SOURCE PORT octets	DEST MSS PORT ADJUST	SYSTE	M IP	LOCAL	COLOR	REMOT	E COLOR
ipsec 1442	192.168 133	8.10.232 22743	192.168.9 0	.233 0	12346	12346 1362	10.10	.10.23	3 biz-i	nternet	biz-i	nternet
BFD	BFD						BFD	BFD	BFD	BFD	BFD	BFD
							ECHO	ECHO	ECHO	ECHO	PMTU	PMTU
PMTU TUNNEL TX	PMTU RX				SOURCE	DEST	TX	RX	ТХ	RX	TX	RX
PROTOCOI OCTETS	L SOURCE OCTETS	IP	DEST IP		PORT	PORT	PKTS	PKTS	OCTETS	OCTETS	PKTS	PKTS
ipsec 0	192.16 0	8.10.232	192.168.9	.233	12346	12346	133	0	22743	0	0	0
vEdge1# 192.168.	show tuni .9.233	nel stati	stics dest	-ip 1	92.168.9	9.233 ;	show t	unnel	statisti	cs bfd d	lest-ip	
TCP TUNNEL TUNNEL PROTOCOI MTU	SOURCE	IP tx-octet	DEST IP s rx-pkts	rx-	SOURCE PORT octets	DEST MSS PORT ADJUST	SYSTE	M IP	LOCAL	COLOR	REMOT	E COLOR
ipsec	192.16	8.10.232	192.168.9	.233	12346	12346	10.10	.10.23	3 biz-i	nternet	biz-i	nternet

1442 134 22914 0 0	1362
--------------------	------

					BFD	BFD	BFD	BFD	BFD	BFD
BFD	BFD				FCHO	FCHO	FCHO	FCHO	דזייזעס	זיייאס
PMTU	PMTU				LCIIO	LCIIO	LCHO	LCHO	FMIO	FMIO
TUNNEL			SOURCE	DEST	TΧ	RX	TΧ	RX	TX	RX
TX	RX									
PROTOCOI	L SOURCE IP	DEST IP	PORT	PORT	PKTS	PKTS	OCTETS	OCTETS	PKTS	PKTS
OCTETS	OCTETS									
ipsec	192.168.10.232	192.168.9.233	12346	12346	134	0	22914	0	0	0
0	0									

#### BFD가 작동 중인 경우:

TCP

vEdge1# show tunnel statistics dest-ip 192.168.9.233 ; show tunnel statistics bfd dest-ip 192.168.9.233 ;

TUNNEL TUNNEL				SC	OURCE	DEST MSS						
PROTOCOI MTU	L SOURCE tx-pkts	IP tx-octet:	DEST IP s rx-pkts	PC rx-oct	ORT tets	PORT ADJUST	SYSTE	M IP	LOCAL	COLOR	REMOTI	E COLOR
ipsec 1441	192.168 3541	8.10.232 610133	192.168.9.2 3504	233 12 592907	2346 7	12346 1361	10.10	.10.23	3 biz-i	nternet	biz-i	nternet
BFD	BFD						BFD	BFD	BFD	BFD	BFD	BFD
דזישעט	DMITT						ECHO	ECHO	ECHO	ECHO	PMTU	PMTU
TUNNEL TX	RX			SC	OURCE	DEST	ТΧ	RX	TX	RX	TX	RX
PROTOCOI OCTETS	L SOURCE OCTETS	IP	DEST IP	PC	ORT	PORT	PKTS	PKTS	OCTETS	OCTETS	PKTS	PKTS
ipsec 20163	192.168 8091	8.10.232	192.168.9.2	233 12	2346	12346	3522	3491	589970	584816	19	13
vEdge1# 192.168.	show tunn .9.233 ;	nel stati:	stics dest-i	ip 192.	.168.9	.233 ;	show t	unnel	statisti	cs bfd d	est-ip	
TCP TUNNEL TUNNEL PROTOCOI	L SOURCE	IP	DEST IP	SC	OURCE	DEST MSS PORT	SYSTE	M IP	LOCAL	COLOR	REMOTI	E COLOR
MTU 	tx-pkts	tx-octet:	s rx-pkts	rx-oct	tets 	ADJUST						

ipsec 192.168.10.232 192.168.9.233 12346 12346 10.10.10.233 biz-internet biz-internet 1441 3542 610297 3505 593078 1361

					BFD	BFD	BFD	BFD	BFD	BFD
BFD	BFD									
					ECHO	ECHO	ECHO	ECHO	PMTU	PMTU
PMTU	PMTU									
TUNNEL			SOURCE	DEST	ΤX	RX	TX	RX	TX	RX
TX	RX									
PROTOCOL	L SOURCE IP	DEST IP	PORT	PORT	PKTS	PKTS	OCTETS	OCTETS	PKTS	PKTS
OCTETS	OCTETS									
ipsec	192.168.10.232	192.168.9.233	12346	12346	3523	3492	590134	584987	19	13
20163	8091									

**참고:**위 출력을 확인하여 BFD 패킷 크기를 캡슐화와 함께 결정할 수 있습니다. 두 출력 간에 하나의 BFD 패킷만 수신되었으므로 BFD Echo RX Octets 값 584987 - 584816을 부스트하면 171바이트 결과가 제공됩니다.BFD 자체에서 사용하는 대역폭을 정확하게 계산하는 것이 유 용할 수 있습니다.

BFD가 **다운** 상태로 중단된 이유는 MTU가 아니라 NAT 컨피그레이션입니다.이는 **작업 시나리오**와 실패 시나리오 간에 변경된 유일한 **사항입니다**.DIA 컨피그레이션의 결과로, 데이터 플레인 IPSec 트래픽 우회를 허용하기 위해 변환 테이블에서 vEdge2에 의해 NAT 고정 매핑이 자동으로 생성되 었음을 여기에서 확인할 수 있습니다.

vEdge2# show ip nat filter nat-vpn 0 nat-ifname ge0/1 vpn 0 protocol udp 192.168.9.233 198.51.100.232

		PRI	IVATE		PRIVATE	PRIVATE		
PUBLIC PUBL	JIC							
NAT NAT		SOU	JRCE	PRIVATE DEST	SOURCE	DEST	PUBLIC S	OURCE
PUBLIC DEST	SOURCE	DEST	FILTER	IDLE	OUTBOUND	OUTBOUND	INBOUND	INBOUND
VPN IFNAME	VPN PROTC	COL ADI	DRESS	ADDRESS	PORT	PORT	ADDRESS	
ADDRESS	PORT	PORT	STATE	TIMEOUT	PACKETS	OCTETS	PACKETS	OCTETS
DIRECTION								
0 ge0/1	0 udp	192	2.168.9.233	198.51.100.23	2 12346	52366	192.168.	9.233
198.51.100.2	232 12346	52366	establish	ned 0:00:00:59	53	8321	0	0 –

# 보시다시피 포트 52366이 42366 대신 사용되고 있습니다. vEdge2는 52366 포트를 예상하여 vSmart에서 광고하는 OMP TLOC에서 이를 학습했기 때문입니다.

vEdge2# show omp tlocs ip 10.10.10.232 | b PUBLIC

PUBLIC	PRIVATE								
ADDRESS								PSEUDO	
PUBLIC		PRIVATE	PUBLIC	IPV6	PRIVATE	IPV6	BFD		
FAMILY	TLOC IP	COLOR		ENCAP	FROM PEEF	ξ	STATUS	KEY	PUBLIC IP
PORT	PRIVATE IP	PORT	IPV6	PORT	IPV6	PORT	STATUS		
ipv4	10.10.10.232	biz-inte	ernet	ipsec	10.10.10.	228	C,I,R	1	
198.51.1	00.232 52366	192.168.1	0.232	12346	::	0	::	0	down

# 솔루션

### NAT 포트 전달

이러한 유형의 문제에 대한 해결 방법은 간단하게 요약할 수 있습니다.vEdge2 전송 인터페이스에 서 고정 NAT 예외 포트 포워딩을 구성하여 모든 소스의 데이터 평면 연결에 대한 필터링을 강제로 우회할 수 있습니다.

```
vpn 0
interface ge0/1
nat
respond-to-ping
port-forward port-start 12346 port-end 12445 proto udp
private-vpn 0
private-ip-address 192.168.9.233
!
!
!
!
```

12346~12446의 범위는 가능한 모든 초기 포트(12346, 12366, 12386, 12406 및 12426 + portoffset)를 수용합니다. 이에 대한 자세한 내용은 "비디오 구축을 위한 방화벽 포트"를 참조하십시오.

CLI 템플릿 대신 디바이스 기능 템플릿을 사용하는 경우 동일한 기능을 구현하려면 이미지에 표시 된 대로 해당 전송(vpn 0) 인터페이스에 대한 새 VPN 이더넷 기능 템플릿을 업데이트하거나 추가해 야 합니다. 해당 전송(vpn 0) 인터페이스에는 해당 **새 포트 전달 규칙**이 사용됩니다.

≡	cisco vManage				• É	1 <b>1</b> 1	<b>?</b> a	dmin 🔻
	CONFIGURATION   TEMPLATES							
	Device Feature							
*	Feature Template > VPN Interface Ethernet							
**	Basic Configuration Tunnel NAT VRRP	AC	L/QoS ARP	802.1X	Advance	ed		
3	New Port Forwarding Rule							
ŝ								
*	Port Start Range	•	12346					
	Port End Range	۲	12445					
_	Protocol	۲	udp	-				
œ								
	VPN	•	0					
	Private IP	⊕ -	192.168.9.233					
						_		
						Add	Cancel	
		Upda	ate Cancel					

## 명시적 ACL

또한 명시적인 ACL을 사용하는 다른 솔루션도 가능합니다.**정책** 섹션에서 implicit-acl-logging이 구 성된 경우 /var/log/tmplog/vdebug 파일에서 다음 메시지를 확인할 수 있습니다.

local7.notice: Jun 8 17:53:29 vEdge2 FTMD[980]: %Viptela-vEdge2-FTMD-5-NTCE-1000026: FLOW LOG vpn-0 198.51.100.232/42346 192.168.9.233/12346 udp: tos: 192 inbound-acl, Implicit-ACL, Result: denyPkt count 2: Byte count 342 Ingress-Intf ge0/1 Egress-intf cpu

#### 근본 원인을 설명하므로 vEdge2의 ACL(Access Control List)에서 다음과 같이 수신 데이터 플레인 패킷을 명시적으로 허용해야 합니다.

```
vpn 0
interface ge0/1
 ip address 192.168.9.233/24
 nat
  respond-to-ping
  1
 tunnel-interface
  encapsulation ipsec
  color biz-internet
  no allow-service bgp
  no 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
  !
          1506
 mtu
 no shutdown
 access-list DATA_PLANE in
 Ţ
1
policy
implicit-acl-logging
access-list DATA_PLANE
 sequence 10
  match
destination-port 12346 12445 protocol 17 ! action accept ! ! default-action drop ! !
디바이스 기능 템플릿을 사용 중인 경우 현지화된 정책을 생성하고 액세스 제어 목록 구성 마법사
단계에서 ACL을 구성해야 합니다.
```

≡	cisco Cisco vMan	nage						•	Ê	<b>_</b> 200	0	admin 👻
::		I   POLICIES	Localized Policy	> Access (	Control Lists Policy	> Edit IPV4 AC	L Policy					
▣	Name	DATA_PLAN	١E									
٠	Description	policy to all	ow data plane traffic									
عر												
A	Add ACL Sequer	nce 🙎	Access Cont	trol List							Access	s Control List
-	↑ Drag & drop to rec	order 🕈	Sequence Rule	Drag and d	lrop to re-arrange rule	S						
÷	Access Control List	: 0										~
11.	Default Action		■ Match Condi	itions				Actions				
			Protocol:		17			Accept				
			✓ Destination:	Port	12346-12445							Î
	PREVIEW				Save A	ACL Policy	CANCEL					

암시적 **acl-logging이** 아직 활성화되지 않은 경우, Save Policy(정책 **저장)** 버튼을 클릭하기 전에 마 지막 단계에서 이를 활성화하는 것이 좋습니다.

≡	Cisco vMana	e	٠	ê	<b>*</b> 10	0	admin 👻	
::	CONFIGURATION   POLICIES Localized Policy > Add Policy							
▣	📀 Create G	🧭 Create Groups of Interest 🤡 Configure Forwarding Classes/QoS 🤄 Configure Access Control Lists 🤡 Configure Route Policy 🧿 Policy Overview						
٠	Enter name and description for your localized master policy							
٩	Policy Name	LOCAL_POLICY						
÷	Policy Description vEdge local policy to allow data plane traffic							
*	Policy Settings							
	Netflow Application Cloud QoS Cloud QoS Service side 🖌 Implicit ACL Logging							
	Log Frequency Enter in seconds (maximum 2147483647)							
	BACK	Preview Save Policy CANCEL						

지역화된 정책(LOCAL_POLICY의 경우)은 디바이스 템플릿에서 참조되어야 합니다.

≡	Cisco vManage			
	CONFIGURATION   TEMPL	ATES		
	Basic Information	Transport & Management VPN	Service VPN	Additional Templates
<b>Å</b>				
a	Additional Templates			
<b>`</b>	Banner	Choose	•	
	Policy	LOCAL_POLICY	•	
1.	SNMP	Choose	•	
1.	Security Policy	Choose	•	
			Cr	eate Cancel

그런 다음 ACL(**DATA_PLANE**라는 이름의 경우)을 인그레스(in) 방향으로 VPN 인터페이스 이더넷 기능 템플릿 아래에 적용해야 합니다.

≡	cisco vManage	
	CONFIGURATION   TEMPLATES	
	Device Feature	
~	Feature Template > Add Template > VPN Interface Ethernet	
**	Basic Configuration Tunnel NAT	VRRP ACL/QoS ARP 802.1X Advanced
ع	ACL/QOS	
ĉ		
*	Shaping Rate (Kbps)	♥ •
	QoS Map	<b>0</b> -
_	doo map	
	Rewrite Rule	⊘ -
	Ingress ACL - IPv4	
	IPv4 Ingress Access List	DATA_PLANE
		Save Cancel

ACL을 구성하고 인터페이스에 적용하여 데이터 플레인 트래픽을 우회하면 BFD 세션은 다시 up 상 태에 도달합니다. TCP TUNNEL SOURCE DEST TUNNEL MSS PROTOCOL SOURCE IP DEST IP PORT PORT SYSTEM IP LOCAL COLOR REMOTE COLOR MTU tx-pkts tx-octets rx-pkts rx-octets ADJUST _____ _____ 192.168.9.233 198.51.100.232 12346 42346 10.10.10.232 biz-internet biz-internet ipsec 1441 1768 304503 1768 304433 1361 REMOTE TLOC SOURCE TLOC DST PUBLIC DETECT TX DST PUBLIC SYSTEM IP SITE ID STATE COLOR COLOR SOURCE IP ΙP PORT ENCAP MULTIPLIER INTERVAL(msec) UPTIME TRANSITIONS _____ _____ 10.10.10.232 biz-internet biz-internet 232 up 192.168.9.233 52346 ipsec 7 1000 198.51.100.232 0:00:14:36 0

## 기타 고려 사항

ACL의 해결 방법은 NAT 포트 전달 방식보다 훨씬 더 실용적입니다. 또한 보안 강화를 위해 원격 사 이트의 소스 주소를 기준으로 매칭할 수 있으며 DDoS 공격으로부터 디바이스로 보호할 수 있습니 다(예:

```
access-list DATA_PLANE

sequence 10

match

source-ip 198.51.100.232/32

destination-port 12346 12445

protocol 17

!

action accept

!
```

또한 다른 수신 트래픽(**allowed-services**로 지정되지 않음)에 대해서도 이 예와 같이 기본 **iperf** 포트 5001 명시적 ACL **시퀀스 20**에 대해서는 데이터 평면 트래픽과 달리 아무런 영향도 미치지 않습니 다.

```
policy
access-list DATA_PLANE
 sequence 10
  match
   source-ip 198.51.100.232/32
   destination-port 12346 12445
                 17
   protocol
  1
  action accept
  !
  1
 sequence 20
  match
   destination-port 5001
              6
   protocol
```

```
!
action accept
!
!
```

# 또한 iperf가 작동하려면 NAT 포트 전달 예외 규칙이 필요합니다.

```
vEdgeCloud2# show running-config vpn 0 interface ge0/1 nat

vpn 0

interface ge0/1

nat

respond-to-ping

port-forward port-start 5001 port-end 5001 proto tcp

private-vpn 0

private-ip-address 192.168.9.233

!

!

?

결혼
```

이는 NAT 소프트웨어 설계 세부 사항으로 인해 vEdge 라우터에서 예상되는 동작이며 피할 수 없습니다.