

تانايب لايوتسم تالاصت اءاطخا فاشكتسا vEdge ل هاجتالايئانث هيچوتلا ءءاعا فشكو اهحالص او

تايوتحمل

[ءمدقملا](#)

[ءيساس الابلطتملا](#)

[تابلطتملا](#)

[ءمدختسملا تانوكوملا](#)

[مكحتلا يوتسم تامولعم](#)

[مكحتلا رصنع لءملحملل صئاصءلا نم ققحتلا](#)

[مكحتلا تالاصتاصف](#)

[بكارتملا ءرادا لوكوتوب](#)

[vEdges لالخ نم \(OMP\) تنرتنالا لوصولا يف مكحتلا تاءونع نالءالا نم ققحتلا](#)

[\(TLOCs\) لقتنالا لوصولا يف مكحتلا تاءونع نالءالا ومليتسي vSmart نأ نم ققحتلا](#)

[هاجتالايئانث هيچوتلا ءءاعا فاشكتسا](#)

[بمأ ءسلج bfd ضرءلا مهفي](#)

[بمألل قفنللا ضرءلا صئاصءلا](#)

[لوصولا ءمئاق](#)

[ءكبشلا ناوئع ءمءرت](#)

[ءيفصتلا لءمءوعو NAT طئارء فاشكتسا stun-client تاوؤا ماءءتسا ءيفي](#)

[CLI يف ءمدختسملا "لاسزالا" تانايبلا يوتسم قافنأل ءمءءملا NAT ءاونأ](#)

[ءياملحلا نارءء](#)

[نامألا](#)

[اهيلاء DSCP ءملاء ءضومت يئالا تانايبلا رورم ءءءء عم ISP لكاشم](#)

[Debug BFD](#)

[ءلص تاؤتاملعم](#)

ءمدقملا

نكلومكحت يوتسم لاصتا ءعب vEdge تانايب يوتسم لاصتا لكاشم دنءتسملا اءه فصفي
ءقءوملا نيب تانايب يوتسم لاصتا ءءوي ال

ءيساس الابلطتملا

تابلطتملا

لءلا Cisco Software Defined Wide Area Network (SDWAN) ءفرعمب Cisco يءصوت

ةمدختسمل تانوكمل

ةيساسأل vEdge مةظنأ لىل دننسسمل اذه زكري .ةني عم ةي دام تانوك م و ج م ارب تارادصا لىل دننسسمل اذه رصتقي ال

ةمدختسُمل ةزهأل ا عي م ج ت ا د ب .ةصاخ ةيل م عم ةئي ب ي ف ةدو ج و م ل ةزهأل ا نم دننسسمل اذه ي ف ةدراول ا تامول عم ل ا عاشن ا م ت ي أ ل م ت ح م ل ر ي ث أ ت ل ل ك م ه ف ن م د ك أ ت ف ، ل ي غ ش ت ل د ي ق ك ت ك ب ش ت ن ا ك ا ذ ا . (ي ض ا ر ت ف ا) ح و س م م ن ي و ك ت ب دننسسمل اذه ي ف ر م أ .

. ةءارق ل ا ج ر ي ، (م ك ح ت ل ا ة د ح و ع و ي ف Cisco IOS® XE ت ا ه ج و م) Cisco Edge ت ا ه ج و م ل

م ك ح ت ل ا ي و ت س م ت ا م و ل ع م

م ك ح ت ل ا ر ص ن ع ل ة ي ل ح م ل ا ص ن ا ص ل خ ل ا ن م ق ق ح ت ل ا

show control local-properties wan-interface-list. ر م أ ل ا م د خ ت س أ ، vEdge لىل ت ا ه ج و ل ا Wide Area Network (WAN) ة ل ا ح ن م ق ق ح ت ل ل

RFC 4787 Network Address Translation (NAT) Type. ة ي ر ك ن ك م ي ، ج ا ر خ ل ا اذه ي ف

User Datagram Protocol (UDP) م ا د خ ت س ا م ت ي ، ص ا خ ل ا و م ا ع ل ا IPv4 ن ا و ن ع و ، (ك ل ذ ل ا ا م و ، ه ج و م ل ا ، ة ي ا م ح ل ا ر ا د ج) NAT ز ا ه ج ف ل خ vEdge ن و ك ي ا م د ن ع . ت ا ن ا ي ب ل ا ي و ت س م ق ا ف ن ا ء ا ش ن ا ل ة ص ا خ ل ا و ة م ا ع ل ا ر د ص م ل ا ذ ف ا ن م (UDP)

ا ه ن ي و ك ت م ت ي ت ل ا م ك ح ت ل ا ت ا ل ا ص ت ا د د ع ل ص ق أ ل ا د ح ل ن و ل و ق ف ن ل ا ة ه ج و ة ل ا ح لىل ر و ث ع ل ا ا ض ي أ ك ن ك م ي .

vEdge1# show control local-properties wan-interface-list NAT TYPE: E -- indicates End-point independent mapping A -- indicates Address-port dependent

ك ن ك م ي ي ت ل ا ذ ف ا ن م ل ا م و ت ا ن ا ي ب ل ا ق ا ف ن ا ء ا ش ن ا ة ي ف ي ك ل و ح ة ن ي ع م ت ا م و ل ع م د ي د ح ت ك ن ك م ي ، ت ا ن ا ي ب ل ا ه ذ ه م ا د خ ت س ا ب . ت ا ن ا ي ب ل ا ق ا ف ن ا ن ي و ك ت د ن ع م ا د خ ت س ل ل (ت ا ه ج و م ل ا ر و ط ن م ن م) ا ه ع ق و ت

م ك ح ت ل ا ت ا ل ا ص ت ا ص ح ف

ي ف م ك ح ت ل ا ت ا د ح و ع م ه ؤ ا ش ن ا م ت م ك ح ت ل ا ص ت ا ه ي د ل ت ا ن ا ي ب ل ا ي و ت س م ق ا ف ن ا ل ك ش ي ا ل ي ذ ل ا ن و ل ل ا ن ا ن م د ك أ ت ل م ه م ل ا ن م . ة ي ش غ ت ل ا

Overlay Management Protocol ر ب ع vSmart ج م ا ن ر ب لىل ت ا م و ل ع م ل ا Transport Locator (TLOC) ل ا س ر ا ب vEdge م و ق ي ن ل ف ، ا ل ا و (OMP).


ء ل ا ح ل a connect ن ع ش ح ب ل ا و ، ر م أ ل a show control connections م ا د خ ت س ا ب ل ي غ ش ت ل ا د ي ق ن ا ك ا ذ ا ا م م ق ق ح ت ل ا ك ن ك م ي .

vEdge1# show control connections PEER PEER CONTROLLER PEER PEER PEER SITE DOMAIN PEER PRIV PEER PUB GROUP TYPE PROT SY

. ن و ل ل ا اذه ر ب ع م ك ح ت ل ا ت ا ل ا ص ت ا ل ح ج ا ن ع د ب ل ا ل خ ن م ا ه ل ح ب م ق ف ، ل ا ص ت ا ل ا (ت ا ن ا ي ب ق ا ف ن ا ل ك ش ت ا ل ي ت ل ا) ة ه ج و ل ا ت ل و ا ح ا ذ ا

. ق ف ن ل ا ة ه ج و م س ق ت ح ت ة د ح م ل ا ة ه ج و ل ا ي ف max-control-connections 0 ن ي ي ع ت ب م ق ، و أ

vpn 0 interface ge0/1 ip address 10.20.67.10/24 tunnel-interface encapsulation ipsec color mpls restrict max-control-connections 0 no allow-service bgp all

 اذه موقوي ال ،كلذ عمو .فدهال س فن قيقحتل رمأل **no control-connections** مادختسا كنكمي ،نايحلأا ضعب يف :عظالم
جماربالا ىلع همادختسا متي الو 15.4 رادصالا نم رمأل اذه لامه مت .مكحتلا تالاصتا ددعل ىصقأل دحلا عاشناب رمأل
ثدحأل.

بكارتلا قرادا لوكوتورب

vEdges لال خ نم (OMP) تنرتنالا ىلى لوصولا يف مكحتلا تادحو نع نالعالا نم ققحتلا

اذه ربع مكحتلا تالاصتا نيوكت لواحت ههجالا نأل (OMP) ةساسألا ةينبالا ىلى لوصولا يف مكحتلا مئاق لاسرا نكمي ال
مكحتلا تادحو ىلى لوصولا هانكمي الو نوللا

نوللا اذهل (TLOC) لقنلا ىلى لوصولا يف مكحتلا دحو لسري (هب تانايبلا قافنأ موقت يذلا) نوللا ناك اذا امم ققحت
vSmart ىلى نيعلما


نارقالا ىلى اهل لاسرا متي يتلا (TLOCs) لوصولا يف مكحتلا مئاق نم **show omp tlocs advertised** ققحتلل رمأل مدختسا
OMP لوكوتورب

ةنولملا MPLS ةزهجالا vSmart ىلى TLOC ي لاسرا متي مل **gold** و **mpls** ناولألا :لاثم

vEdge1# show omp tlocs advertised C -> chosen I -> installed Red -> redistributed Rej -> rejected L -> looped R -> resolved S -> stale Ext -> extranet Stg

ناولألا نم لكل TLOC لاسرا متي **gold** و **mpls** ناولألا :لاثم

vEdge2# show omp tlocs advertised C -> chosen I -> installed Red -> redistributed Rej -> rejected L -> looped R -> resolved S -> stale Ext -> extranet Stg

 0.0.0.0 ىلع **FROM PEER** لقنلا نييعت متي ،مكحتلا ىوتسم نع اي لحم اهؤاشن متي تامولعم يأل ةبسنلاب :عظالم
ةمقلا هذه ىلى اذانتسا ةقباطملا نم دكأت ،اي لحم اهؤاشن مت تامولعم نع ثحبالا دنع

(TLOCs) لقنلا ىلى لوصولا يف مكحتلا تادحو نع نلعي و ملتسي vSmart نأ نم ققحتلا

نم TLOC نيوانع ىقلتي هنأ نم دكأت .vSmart ةكرشل (TLOC) لقنلا ىلى لوصولا يف مكحتلا مئاق نع نالعالا نأل متي
رخألا vEdge ىلى انه نع نلعأو حيحصلا ريظنلا

vEdge1. 10.1.0.2 نم TLOC نيوانع vSmart ملتسي :لاثم

<#root>

vSmart1# show omp tlocs received

C -> chosen I -> installed

Red -> redistributed Rej -> rejected L -> looped

R -> resolved

S -> stale Ext -> extranet Stg -> staged Inv -> invalid PUBLIC PRIVATE ADDRESS PSEUDO PUBLIC PRIVATE P

10.1.0.2 mpls ipsec 10.1.0.2 C,I,R 1 10.20.67.20 12386 10.20.67.20 12386 :: 0 :: 0 -

10.1.0.2 blue ipsec 10.1.0.2 C,I,R 1 198.51.100.187 12406 10.19.146.2 12406 :: 0 :: 0 -

10.1.0.30 mpls ipsec 10.1.0.30 C,I,R 1 10.20.67.30 12346 10.20.67.30 12346 :: 0 :: 0 - 10.1.0.30 gold

هذه نم ققحت ،انه ىرخأ زومر ىأ ىرت وأ TLOCs ىرت مل اذا

<#root>

vSmart-vIPtela-MEX# show omp tlocs received

C -> chosen

I -> installed

Red -> redistributed

Rej -> rejected

L -> looped

R -> resolved

S -> stale Ext -> extranet Stg -> staged

Inv -> invalid

PUBLIC PRIVATE ADDRESS PSEUDO PUBLIC PRIVATE PUBLIC IPV6 PRIVATE IPV6 BFD FAMILY TLOC IP COLOR ENCAP F

10.1.0.2 mpls ipsec 10.1.0.2 C,I,R 1 10.20.67.20 12386 10.20.67.20 12386 :: 0 :: 0 -

10.1.0.2 blue ipsec 10.1.0.2 Rej,R,Inv 1 198.51.100.187 12406 10.19.146.2 12406 :: 0 :: 0 -

10.1.0.30 mpls ipsec 10.1.0.30 C,I,R 1 10.20.67.30 12346 10.20.67.30 12346 :: 0 :: 0 - 10.1.0.30 gold

TLOCs رطحب موقى جهن دوجو مدع نم ققحت.

show run policy control-policy - وه امك advertised كب ةصاخلا (TLOCs) لوصولا يف مكحتلا تاودأ ضفرت عولت ةمئاق ىأ نع ثحبا -
received ةىنقت يف وأ vSmart.

<#root>

```
vSmart1(config-policy)# sh config policy lists tloc-list SITE20
```

```
tloc 10.1.0.2 color blue encap ipsec
```

```
!! control-policy SDWAN
```

```
sequence 10 match tloc tloc-list SITE20 ! action reject ---->
```

here we are rejecting the TLOC 10.1.0.2,blue,ipsec !! default-action accept !

```
apply-policy
```

```
site-list SITE20
```

```
control-policy SDWAN in ----->
```

the policy is applied to control traffic coming IN the vSmart, it will filter the tlocs before adding i



منع نالعالا متي الف، كذلك ناك **Invalid** و **Rejected** (TLOC) لقنلنا لى لوصولنا في مكحتلنا تاودأ دحأ ناك اذا: **عظالم** ىرخألأ ةزهألل.

vSmart ىل عهالسا مت TLOC نأ ىرت نأ كنكمي vSmart. نم هنع نالعالا دنع TLOC ةيفصت ب موقت ال ةسايسلا نأ نم دكأت ىرخألأ vEdge ىل عهتؤر كنكمي ال نكلول.

مثال 1: vSmart عم TLOC في C.I.R.

```
<#root>
```

```
vSmart1# show omp tlocs
```

```
C -> chosen I -> installed
```

```
Red -> redistributed Rej -> rejected L -> looped
```

```
R -> resolved
```

```
S -> stale Ext -> extranet Stg -> staged Inv -> invalid PUBLIC PRIVATE ADDRESS PSEUDO PUBLIC PRIVATE P
```

```
10.1.0.2 mpls ipsec 10.1.0.2 C,I,R 1 10.20.67.20 12386 10.20.67.20 12386 :: 0 :: 0 - 10.1.0.2 blue ipse
```

```
10.1.0.30 mpls ipsec 10.1.0.30 C,I,R 1 10.20.67.30 12346 10.20.67.30 12346 :: 0 :: 0 - 10.1.0.30 gold
```

مثال 2: TLOC MPLS ال ىرت ال vEdge2 نم يتأي قرزأ نول نم TLOC نول vEdge1 ىري ال.

```
<#root>
```

```
vEdge1# show omp tlocs C -> chosen I -> installed Red -> redistributed Rej -> rejected L -> looped R -> resolved S -> stale Ext -> extranet Stg -> staged I
```

```
10.1.0.2 mpls ipsec 10.1.0.3 C,I,R 1 10.20.67.20 12386 10.20.67.20 12386 :: 0 :: 0 up
```

```
10.1.0.30 mpls ipsec 10.1.0.3 C,I,R 1 10.20.67.30 12346 10.20.67.30 12346 :: 0 :: 0 up 10.1.0.30 gold
```

vEdge1 ىل عهالسا TLOC روهظ مدع ببس ةظالم كنكمي، جهنلنا نم ققحتلنا ب موقت ام دنع

<#root>

```
vSmart1# show running-config policy policy lists tloc-list SITE20
```

```
tloc 10.1.0.2 color blue encap ipsec
```

```
! site-list SITE10 site-id 10 ! ! control-policy SDWAN sequence 10 match tloc
```

```
tloc-list SITE20
```

```
! action reject ! ! default-action accept !
```

```
apply-policy
```

```
site-list SITE10
```

```
control-policy SDWAN out
```

```
!
```

```
!
```

هإچتالال ینئانث هیجوتال اءاع | فاشتك

رمأ قسلج bfd ضرعلأ مهفې

جئاتنالل ېف اهنع ثحبن نأ انېل ع نېع تې ېتال اءېساسأل اءاېشأل ېه هءه:

<#root>

```
vEdge-2# show bfd sessions SOURCE TLOC REMOTE TLOC DST PUBLIC DST PUBLIC DETECT TX SYSTEM IP SITE ID STATE COLOR COLOR
```

```
10.1.0.5 10 down blue gold 10.19.146.2 203.0.113.225 4501 ipsec 7 1000 NA 7
```

```
10.1.0.30 30 up blue gold 10.19.146.2 192.0.2.129 12386 ipsec 7 1000 0:00:00:22 2 10.1.0.4 40 up blue
```

```
10.1.0.4 40 up mpls mpls 10.20.67.10
```


- **SYSTEM IP:** تئرنئالال لوكوتورب - اءرظئالال ماظن
- **SOURCE and REMOTE TLOC COLOR:** هل سرتو TLOC هاقلئت نأ ع قوتې ام ءفرعم ءېفم ال نم.
- **SOURCE IP:** عم تېأرئت نك عېطتسې وه) انه ضرع ءمولعم اءه، NAT اءارو تئان نوكې ن | IP رءصم private وه **show control local-properties <wan-interface-list>** نم لالام عئسألال
- **DST PUBLIC IP:** لال: ام) ال. مأل NAT اءارو ناك اءوس، قفنل **Data Plane** لېكشئتل VEdge اهم ءختسې ېتال ءهءولل ېه **DST PUBLIC IP** (تاطابئرالال **Multi-Protocol Label Switching (MPLS)** و، تئرنئالال اءرشابم ءلصئت VEdges
- **DST PUBLIC PORT** ال قفنل **Data Plane** لېكشئتل VEdge وه ءختسې ماع NAT-ed ءفم **DST PUBLIC PORT** ءېعبلال VEdge ال قفنل | قفنل **Data Plane** لېكشئتل VEdge وه ءختسې ماع NAT-ed ءفم
- **TRANSITIONS:** سلكل او UP ال NA نم ىءئئم لال لمع ءسلج اءېف ترفېغ ېتال تارم لال ءءع

رمألل قفنل اضرع تايئاصح!

مزح ملتست وأ لسرت تنك اذا ام ديدحت كنكمي . تانايبل يوتسم قافنأ لوح تامولعمل اضرع نأ **show tunnel statistics** نكمي
قفل IPSec نمي ني عم vEdges.

دقعل ني لاصلتالا لكاشم لزعو ، ةيانهن لك لصلت مزحل تنك اذا ام مهف يلع كلذ كدعاسي نأ نكمي .

rx-pkts وأ **tx-pkts** يف ةدايز ال وأ ةدايز ةطحال م كنكمي ، تارم ةدع رمال ليغشش تب موقت ام دنع ، لاثملا يف

 ينعي اذهف ، RX-PKTS ديازتي مل اذا . ريظنلا لاي تانايبل لقنت كنإف ، tx-pkts ةدايزل كب صاخلا دادعل نك اذا : حيملت
tx-pkts ةدايز نم دكأتو رخآلا فرطلا نم ققحت ، ثدحل اذه يف . ريظنلا نم تانايبل يقلت متي ال هنا

<#root>

TCP vEdge2# show tunnel statistics

```
TUNNEL SOURCE DEST TUNNEL MSS PROTOCOL SOURCE IP DEST IP PORT PORT SYSTEM IP LOCAL COLOR REMOTE COLOR MTU tx-
ipsec 172.16.16.147 10.88.244.181 12386 12406 10.1.0.5 public-internet default 1441 38282 5904968 38276
ipsec 172.16.16.147 10.152.201.104 12386 63364 10.1.0.0 public-internet default 1441 33421 5158814 334
```

TUNNEL PROTOCOL	SOURCE IP	DEST IP	SOURCE PORT	DEST PORT	SYSTEM IP	LOCAL COLOR	REMOTE COLOR	MTU
ipsec	172.16.16.147	10.88.244.181	12386	12406	10.1.0.5	public-internet	default	38276
ipsec	172.16.16.147	10.152.201.104	12386	63364	10.1.0.0	public-internet	default	33421
ipsec	172.16.16.147	10.152.204.31	12386	58851	10.1.0.7	public-internet	public-internet	38276
ipsec	172.24.90.129	10.88.244.181	12426	12406	10.1.0.5	biz-internet	default	38276
ipsec	172.24.90.129	10.152.201.104	12426	63364	10.1.0.0	biz-internet	default	33421
ipsec	172.24.90.129	10.152.204.31	12426	58851	10.1.0.7	biz-internet	public-internet	38276

نمض ملتسي ول سري طبر BFD نم مقرلا صحفي نأ تلمعتسا تنك عيطتسي نأ **show tunnel statistics bfd** وه ديفم رخآ رمأ
صاخ قفن يوتسم تانايبل :

```
vEdge1# show tunnel statistics bfd BFD BFD BFD BFD BFD BFD PMTU PMTU PMTU PMTU TUNNEL SOURCE DEST ECHO TX ECHO RX BFD
```

لوصولا ةمئاق

تاجرخل **show bfd sessions** لاي رظنت نأ دعب ةيروزو ةديفم ةوطخ يه لوصولا ةمئاق .

لباقم ةقباطم **Access Control List (ACL)** عاشن كنكمي ، ةفورعم ةماعلاو ةصاخلا ذفانملاو IP نيوانع تحبصأ نأ دعب نآلا
SRC_Port و DST_Port و SRC_IP و DST_IP .

ةم لتس م ل او ة لس ر م ل BFD لئ اس ر ن م ق ق ح ت ل ا ف ك ل ذ د ع ا س ي ن ا ن ك م ي .

(ACL) ل و ص و ل ا ي ف م ك ح ت ل ا ة م ئ ا ق ن ي و ك ت ل ل ا ث م ي ل ع ر و ث ع ل ا ك ن ك م ي ، ا ن ه

```
policy access-list checkbfd-out sequence 10 match source-ip 192.168.0.92/32 destination-ip 198.51.100.187/32 source-port 12426 destination-port 12426 !
default-action accept
!
access-list checkbfd-in sequence 20 match source-ip 198.51.100.187/32 destination-ip 192.168.0.92/32 source-port 12426 destination-port 12426 ! action
vpn 0
interface ge0/0
access-list checkbfd-in in
access-list checkbfd-out out
!
!
!
```

م ت ي ي ت ل ا BFD لئ اس ر ع م 10 ل س ل س ت ل ا ق ب ا ط ا ت ي . ن ي ل س ل س ت ه ذ ه (ACL) ل و ص و ل ا ي ف م ك ح ت ل ا ة م ئ ا ق م د خ ت س ت ، ل ا ث م ل ا ي ف
س ك ع ل ا ل ع ف ي 20 ل س ل س ت ل ا . ر ي ظ ن ل ا ل ا vEdge ا ذ ه ن م ا ه ل ا س ر ا

ة ي ا غ و ر د ص م ن ي م ي ص ح ف ي ن ا ت ن م ص ، vEdge NAT ل ل م ع ت س ي ن ا . ا ن ي م (Public) ة ي ا غ و ا ن ي م (Private) ر د ص م ل د ص ق ب ا ط ي و ه
ا ن ي م .

ل ل ق ق ح ت ل ل `show policy access-list counters <access-list name>` ر ا د ص ا ب م ق ، ل س ل س ت د ا د ع ل ك ح ت ا ت ن ن م ق ق ح ت ل ل

```
vEdge1# show policy access-list-counters NAME COUNTER NAME PACKETS BYTES ----- checkbfd bfd-out-t
```

ة ك ب ش ل ل ا ن ا و ن ع ة م ح ر ت

ة ي ف ص ت ل ل ا م ا و ع و NAT ط ئ ا ر خ ف ا ش ت ك ا ل stun-client ت ا و د ا م ا د خ ت س ا ة ي ف ي ك .

UDP NAT Traversal (RFC 4787) Map and Filter د ي د ح ت ي ه ة ي ل ا ت ل ا ة و ط خ ل ا ن ا ف ، NAT ف ل خ ت ن ا و ت ا و ط خ ل ل ك ب ت م ق د ق ت ن ك ن ا
ك . ل و س ل ل **Filter** .

nat. ز ا ه ج ف ل خ ا د و ج و م ا ذ ه vEdge ن و ك ي ا م د ن ع vEdge ي ل ح م ل ا ي ج ر ا خ ل ا IP ن ا و ن ع ف ا ش ت ك ا ل ة ا د ا ل ه ذ ه م د خ ت س ت

stun google ل ا ث م : م ا ع م د ا خ) م د ا خ و ي ل ح م ة ا د ا ل ن ي ب nat ل ل و ح ة ي ص ا خ ا ي ر ا ي ت خ | ف ش ت ك ي و ز ا ه ج ل ل ر س ي ا ط ي ط خ ت ر م ا ا ذ ه ا ق ي ل ت ي
(ل د ا ن) .



ع ق و م ل ا ة ر ا ي ز ي ج ر ي ، ة ي ل ي ص ف ت ل ا ت ا م و ل ع م ل ا ن م د ي ز م ل : ع ظ ح الم [Docs Viptela - STUN Client](#)

<#root>


```
vEdge1# tools stun-client vpn 0 options "--mode full --localaddr 192.168.12.100 12386 --verbosity 2 stunclient --mode full --localaddr 192.168.12.100 stun.l.google.com in VPN 0 Binding test: success
Local address: 192.168.12.100:12386
Mapped address: 203.0.113.225:4501
Behavior test: success
```

Nat behavior: Address Dependent Mapping

Filtering test: success

Nat filtering: Address and Port Dependent Filtering


اليلق ةغايصلا فللخت نأ نكمي ،جم انربلا نم ثدحألا تارادصلا ي:

<#root>

```
vEdge1# tools stun-client vpn 0 options "--mode full --localaddr 192.168.12.100 --localport 12386 --verb
```

Google STUN. مداخل لىل 12386 UDP روصم ذفنم مداخلتساب لم اك NAT فشك رابتحا اارجاب موقت ،لا ثمال اذه ي

RFC 4787 لىل ادا نلسا NAT حشرم عونو NAT كولس رمألا اذه جارخا كحنمي

 **allow-service** مداخلتساب لىل اهان افلاو ،قفلنلا هجاو ي STUN ةمدخل حامسلا **tools stun** ركذت ،مداخلتسالا دنع :ةظالم **stun** قعصلا تانايب ريرمتب حامسلا لىل **stun**.

<#root>

```
vEdge1# show running-config vpn 0 interface ge0/0 vpn 0 interface ge0/0 ip address 10.19.145.2/30 ! tunnel-interface encapsulation ipsec color gold max-
allow-service stun
! no shutdown ! !
```

(UDP ل NAT كولس) RFC 4787 و (طورخملا لم اك NAT) STUN تاحل طصم ني ب ني يعتلا اذه حضوي

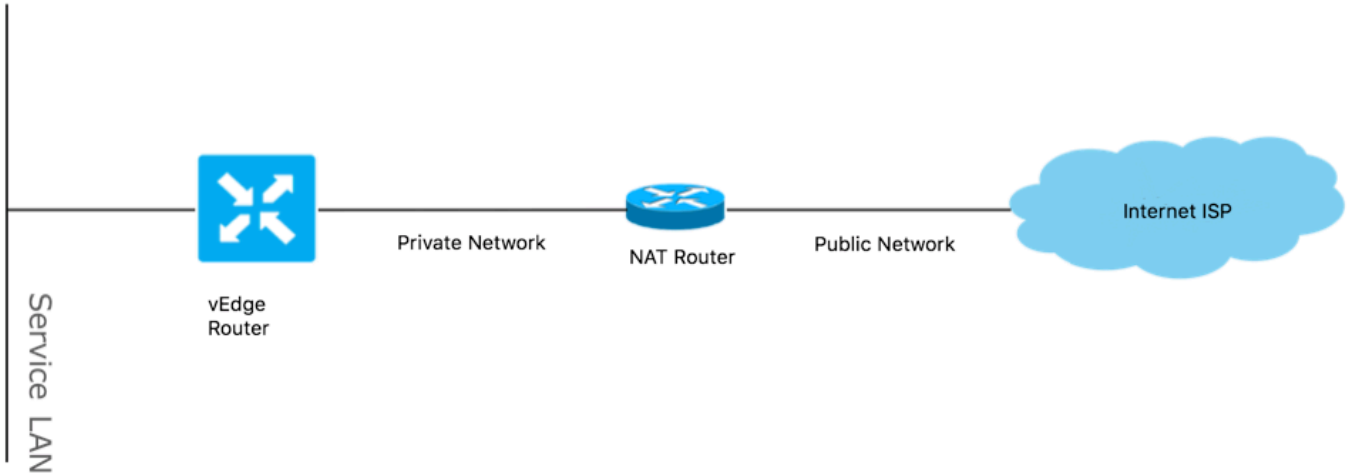
NAT Traversal Mapping Between used Viptela Terminologies		
STUN RFC 3489 Terminology	RFC 4787 Terminology	
	Mapping Behavior	Filtering Behavior
Full-cone NAT	Endpoint-Independent Mapping	Endpoint-Independent Filtering
Restricted Cone NAT	Endpoint-Independent Mapping	Address-Dependent Filtering
Port-Restricted Cone NAT	Endpoint-Independent Mapping	Address and Port-Dependent Filtering
Symmetric NAT	Address-and(or) Port-Dependent Mapping	Address-Dependent Filtering
		Address and Port-Dependent Filtering

CLI يف عم دختس الم "الاسرال" تانايبلا يوتسم قافنأل عم ودم الم NAT عاونأ

تنترنالاب ةرشابم internet-ةماعلا وأ biz-internet لثم ةماعلا كناولأ طبر نمي ،تالاحل مطعم يف

يفل ةماعلا تنترنالاب ةمدخ دوزمو vEdge WAN ةهجاو فلخ nat زاغ كانه ،رخأ تالاح يف

زاغلا وه (كلذ لا امو ،ةيامحل رادجو ،هجوملا) رخألا زاغلا نوكي نأ نم يف و صاخ IP ناونع VEdge ل نوكي نأ نم يف ،ةقيرطلا هذب ةماعلا IP نيوانع لمحي يذلا



هذه قافنأ يوتسم لفيكشت حمسي ال نأ اعويش بابسأل رثكأ دحأ تنك نم كمأ وه كلذ دعب ،عون nat حيحص ريغ تنأ يقلت يف نا ةموعدم الم NAT عاونأ يف

NAT Traversal Support		
Source	Destination	Supported (YES/NO)
Full-Cone NAT	Full-cone NAT	Yes
Full-Cone NAT	Restricted Cone NAT	Yes
Full-Cone NAT	Port-Restricted Cone NAT	Yes
Full-Cone NAT	Symmetric NAT	Yes
Restricted Cone NAT	Full-cone NAT	Yes
Restricted Cone NAT	Restricted Cone NAT	Yes
Restricted Cone NAT	Port-Restricted Cone NAT	Yes
Restricted Cone NAT	Symmetric NAT	Yes
Port-Restricted Cone NAT	Full-cone NAT	Yes
Port-Restricted Cone NAT	Restricted Cone NAT	Yes
Port-Restricted Cone NAT	Port-Restricted Cone NAT	Yes
Port-Restricted Cone NAT	Symmetric NAT	No
Symmetric NAT	Full-cone NAT	Yes
Symmetric NAT	Restricted Cone NAT	yes
Symmetric NAT	Port-Restricted Cone NAT	No
Symmetric NAT	Symmetric NAT	No

ةيامحل نارديج

نأ لمعتسي عانيم الم عنمي ةيامح رادج نأ نم يف وه ،عون ةياغو رديصم موعدم ريغ لا يف سيلو لعفلاب nat لا تنأ صح يف نا قافنأل Data Plane لكشي

تأنيب الواجهة: **vEdge to vEdge Data Plane:**

UDP 12346 إلى 13156

مكثرت الترحيل إلى vEdge من مكثرت الترحيل

UDP 12346 إلى 13156

TCP من 23456 إلى 24156 لوكوتورب

تأنيب الواجهة وتسمي قافل أن حجان لاصتا قيقحتل ذفانم هذه قحتف نم دكأت

show tunnel statistics أو **show bfd sessions | tab** سيلي نكل **show bfd sessions**.
مادختس إكنكمي، تأنيب الواجهة وتسمي قافل أن م دختسم له جولاو رصم الذفانم نم ققحت ام دنع

تأنيب الواجهة وتسمي تن أن أمب انيم ةياغ طقف، انيم رصم يأي دبي ال وه

```
vEdge1# show bfd sessions SOURCE TLOC REMOTE TLOC DST PUBLIC DST PUBLIC DETECT TX SYSTEM IP SITE ID STATE COLOR COLOR
```



[لن](#) م دختسم ال SD-WAN ةياغ راج ذفانم لوح تامولعمل نم ديزم يلع روثعل نكمي: **نظالم**

نامألا

show system statistics تاراركتل نم ديدعل نم ققحتف، رداصل او دراوا ديزي (ACL) لوصول ي ف مكثرتل ةمئاق دادع نأ تظحال اذا **diff** and ensure there are no drops.

<#root>

```
vEdge1# show policy access-list-counters NAME COUNTER NAME PACKETS BYTES -----
```

```
checkbfd bfd-out-to-dc1-from-br1 55 9405
```

```
bfd-in-from-dc1-to-br1 54 8478
```

show system statistics diff command ل راركت لك عم ةدايز **rx_replay_integrity_drops**، جتاننلا اذه ي ف

<#root>

```
vEdge1#show system statistics diff
```

```
rx_pkts : 5741427
```

```
ip_fwd : 5952166
```

```
ip_fwd_arp : 3
```

```
ip_fwd_to_egress : 2965437
```

ip_fwd_null_mcast_group : 26
ip_fwd_null_nhop : 86846
ip_fwd_to_cpu : 1413393
ip_fwd_from_cpu_non_local : 15
ip_fwd_rx_ipsec : 1586149
ip_fwd_mcast_pkts : 26
rx_bcast : 23957
rx_mcast : 304
rx_mcast_link_local : 240
rx_implicit_acl_drops : 12832
rx_ipsec_decap : 21
rx_spi_ipsec_drops : 16

rx_replay_integrity_drops : 1586035

port_disabled_rx : 2
rx_invalid_qtags : 212700
rx_non_ip_drops : 1038073
pko_wred_drops : 3
bfd_tx_record_changed : 23
rx_arp_non_local_drops : 19893
rx_arp_reqs : 294
rx_arp_replies : 34330
arp_add_fail : 263
tx_pkts : 4565384
tx_mcast : 34406
port_disabled_tx : 3
tx_ipsec_pkts : 1553753
tx_ipsec_encap : 1553753
tx_pre_ipsec_pkts : 1553753
tx_pre_ipsec_encap : 1553753
tx_arp_replies : 377
tx_arp_reqs : 34337
tx_arp_req_fail : 2
bfd_tx_pkts : 1553675
bfd_rx_pkts : 21
bfd_tx_octets : 264373160
bfd_rx_octets : 3600
bfd_pmtu_tx_pkts : 78
bfd_pmtu_tx_octets : 53052
rx_icmp_echo_requests : 48
rx_icmp_network_unreach : 75465
rx_icmp_other_types : 47
tx_icmp_echo_requests : 49655
tx_icmp_echo_replies : 48
tx_icmp_network_unreach : 86849
tx_icmp_other_types : 7

vEdge1# show system statistics diff

rx_pkts : 151
ip_fwd : 157
ip_fwd_to_egress : 75
ip_fwd_null_nhop : 3
ip_fwd_to_cpu : 43
ip_fwd_rx_ipsec : 41
rx_bcast : 1

rx_replay_integrity_drops : 41

```
rx_invalid_qtags : 7
rx_non_ip_drops : 21
rx_arp_non_local_drops : 2
tx_pkts : 114
tx_ipsec_pkts : 40
tx_ipsec_encap : 40
tx_pre_ipsec_pkts : 40
tx_pre_ipsec_encap : 40
tx_arp_reqs : 1
bfd_tx_pkts : 40
bfd_tx_octets : 6800
tx_icmp_echo_requests : 1
vEdge1# show system statistics diff
```

```
rx_pkts : 126
ip_fwd : 125
ip_fwd_to_egress : 58
ip_fwd_null_nhop : 3
ip_fwd_to_cpu : 33
ip_fwd_rx_ipsec : 36
rx_bcast : 1
rx_implicit_acl_drops : 1
```

rx_replay_integrity_drops : 35

```
rx_invalid_qtags : 6
rx_non_ip_drops : 22
rx_arp_replies : 1
tx_pkts : 97
tx_mcast : 1
tx_ipsec_pkts : 31
tx_ipsec_encap : 31
tx_pre_ipsec_pkts : 31
tx_pre_ipsec_encap : 31
bfd_tx_pkts : 32
bfd_tx_octets : 5442
rx_icmp_network_unreach : 3
tx_icmp_echo_requests : 1
tx_icmp_network_unreach : 3
vEdge1# show system statistics diff
```

```
rx_pkts : 82
ip_fwd : 89
ip_fwd_to_egress : 45
ip_fwd_null_nhop : 3
ip_fwd_to_cpu : 24
ip_fwd_rx_ipsec : 22
rx_bcast : 1
rx_implicit_acl_drops : 1
```

rx_replay_integrity_drops : 24

```
rx_invalid_qtags : 2
rx_non_ip_drops : 14
rx_arp_replies : 1
tx_pkts : 62
tx_mcast : 1
tx_ipsec_pkts : 24
tx_ipsec_encap : 24
```

```
tx_pre_ipsec_pkts : 24
tx_pre_ipsec_encap : 24
tx_arp_reqs : 1
bfd_tx_pkts : 23
bfd_tx_octets : 3908
rx_icmp_network_unreach : 3
tx_icmp_echo_requests : 1
tx_icmp_network_unreach : 3
vEdge1# show system statistics diff
```

```
rx_pkts : 80
ip_fwd : 84
ip_fwd_to_egress : 39
ip_fwd_to_cpu : 20
ip_fwd_rx_ipsec : 24
```

```
rx_replay_integrity_drops : 22
```

```
rx_invalid_qtags : 3
rx_non_ip_drops : 12
tx_pkts : 66
tx_ipsec_pkts : 21
tx_ipsec_encap : 21
tx_pre_ipsec_pkts : 21
tx_pre_ipsec_encap : 21
bfd_tx_pkts : 21
bfd_tx_octets : 3571
```

ال تنك اذا رظناو **show system statistics diff** تاراركت ةدعب رم ،كلذ دعب vEdge. لىل **request security ipsec-rekey** ا ذيفنتب مق ،الوا
لازت **rx_replay_integrity_drops** ىرت لازت

كب صاخلا نامأل نيوكت نم ققحتف ،كلذب تمق اذا

```
vEdge1# show running-config security security
ipsec
authentication-type sha1-hmac ah-sha1-hmac
!
```

اهيلع **DSCP** ةمالع عضو مت يثلا تانايبلا رورم ةكرح عم **ISP** لكاشم

و **DTLS** تالاصت ا ربع مكحتلا تادحو لىل vEdge هجوم نم ةرادال او مكحتلا تانايب رورم تاكرح عي مج لقتنت ،يضارتفا لكشبو
(ايرشع امقر 48) **CS6** نم **DSCP** ةميقب اهيلع ةمالع عضو متي و **TLS**

اهضعب لىل تانايبلا رورم ةكرح لاسرال **GRE** و **IPsec** ني مضت vEdge تاهجوم مدختست ،تانايبلا ناكم قافنأ رورم ةكرح
ضعبلا

ضعبلا اهضعب **BFD** مزح لاسراب يروء لكشب تاهجوملا موقت ،عادال سايقو تانايبلا يوتسم لشف فاشتكال

(ايرشع امقر 48) CS6 نم DSCP ةميقب هذه BFD مزح زيمي مت اضيأ متي.

vEdge تاهجوم نأل كلذكو CS6 ةميق تاذا DSCP عم UDP رورم ةكرح هنأ يلع رورملا ةكرح نم عونلا اذه ةطحالم متي، ISP روظنم نم يضارتفا لكشب يجراخلال IP سألر يلل تامالع ب موقبي يذلل DSCP لوكوتورب خسنت SD-WAN يف مكحتللا تادحوو.

ةرباعلال ISP هجوم يلل لمعت tcpdump تنالك اذا رمالا ودبي نأ نكمي فيكي يلي امي:

```
14:27:15.993766 IP (tos 0xc0, ttl 64, id 44063, offset 0, flags [DF], proto UDP (17), length 168) 192.168.109.5.12366 > 192.168.20.2.12346: [udp sum ok]
```

مقرلا يواسي يذلل (DS لقلح مساب اضيأ فورعملال TOS Byte 0xc0 ب مزحلل عيجم يلل ةمالع عضو متي، انه هتيؤر نكمي امك ةيئانثلال ميقلالاب 1100000 وأ 192. يرشعلال.

(CS6) وأ يرشعلال مقرلا يفي 48 DSCP تب تادحو ةميق عم قفاوتت ببيترتلال ةيلال تب تادحو 6 لوأ

رورم ةكرح قفن تايطعم يوتسم يلل، يقبي نأ 2 و مكحت يوتسم قفن يلل فداري جاتناللا يفي طبر 2 لوأ

عضو متي (Rx و TX تاهاجت) BFD مزح تنالك اهنأ ةيلال ةقثب جتننتست نأ نكمي اهنإف، TOS ةمالع و ةمزحلل لوظ يلل اذانتسا اضيأ مزحلل هذه يلل CS6 ةمالع.

تايوتسم يلل ظافحلاب (VPN/MPLS L2 VPN/MPLS L3 VPN/MPLS ةمدخ يوزم ةصاخو) ةمدخلل يوزم ضعب موقبي نايجألأ ضعب يفيو فللخم لكشب DSCP تامالع يلل اذانتسا رورملا ةكرح نم ةفللخم ةئف ةجالعم مهنكمي و (SLA) ةمدخلل يوتسم نم ةفللخم

DSCP EF لوكوتورب ربع تاراشلال لاسراو توصلال رورم ةكرح ةيولوأ ديدحتل ةقئاف ةمدخ لكيدل تنالك اذا، لاثملا لبيس يلل CS6.

اذهل، ام طابترال يلامجاللا يددرتلال قاطنلال زواجت متي مل اذا يتح، تددح ابيرقت مئاد لكشب نوكبي رورم ةكرح ةيولوأ نأ امب اضيأ ةفربر BFD تاسلج نوكت نأ نكمي يلالالابو، اهتيؤر نكمي ةمزحلل نادق رورم ةكرح نم عونلال

تالاج ييأ يرت نلف، ةمدخلل دوزم هجوم يلل ةصصخملا ةيولوالأ راطت نا ةمئاق عيوجت مت اذا هنأ تالاحلل ضعب يفي ظحول دقو (vEdge) هجوم نم طيسبلا لاصتالا رابتلخ لايغشت دنع، لاثملا لبيس يلل) ةيداعلال رورملا ةكرحل طوقس

(TOS تيباب) انه اهتيؤر نكمي امك 0 ةيضارتفالال DSCP ةميقب هذه رورملا ةكرح يلل ةمالع عضو متي هنأل كلذو

```
15:49:22.268044 IP (tos 0x0, ttl 62, id 0, offset 0, flags [DF], proto UDP (17), length 142) 192.168.110.5.12366 > 192.168.109.7.12346: [no cksum] UDP,
```

ةفربرت كب ةصاخلال BFD تاسلج ناف، تقوللا سفن يفي نكلو

```
show bfd history DST PUBLIC DST PUBLIC RX TX SYSTEM IP SITE ID COLOR STATE IP PORT ENCAP TIME PKTS PKTS DEL -----
```

تيرحت in order to ديفم طيقتنلالا يتأي انهو

```
vedge2# tools nping vpn 0 options "--tos 0x0c --icmp --icmp-type echo --delay 200ms -c 100 -q" 192.168.109.7 Nping in VPN 0 Starting Nping 0.6.47 ( ht
```

Debug BFD

إذا تم تكوين vEdge مع BFD، فسيتم تشغيل BFD تلقائيًا عند بدء تشغيل vEdge.

يتم تشغيل `debug ftm bfd` على vEdge لتتبع BFD. يمكن تشغيل `debug ftm bfd` على vEdge لتتبع BFD (FTM) عند بدء تشغيل vEdge.

يتم تشغيل `debug ftm bfd` على vEdge لتتبع BFD. يمكن تشغيل `debug ftm bfd` على vEdge لتتبع BFD (FTM) عند بدء تشغيل vEdge. يمكن تشغيل `debug ftm bfd` على vEdge لتتبع BFD (FTM) عند بدء تشغيل vEdge.

يمكن تشغيل `debug ftm bfd` على vEdge لتتبع BFD (FTM) عند بدء تشغيل vEdge. يمكن تشغيل `debug ftm bfd` على vEdge لتتبع BFD (FTM) عند بدء تشغيل vEdge.

يتم تشغيل `debug ftm bfd` على vEdge لتتبع BFD (FTM) عند بدء تشغيل vEdge. يمكن تشغيل `debug ftm bfd` على vEdge لتتبع BFD (FTM) عند بدء تشغيل vEdge.

```
log:local7.debug: May 7 16:23:09 vedge2 FTMD[674]: bfdmgr_session_update_state[1008]: BFD-session TNL 192.168.110.5:12366->192.168.110.6:123
```

يتم تشغيل `debug ttm events` على vEdge لتتبع Tunnel Traffic Manager (TTM) عند بدء تشغيل vEdge.

يتم تشغيل `debug ttm events` على vEdge لتتبع Tunnel Traffic Manager (TTM) عند بدء تشغيل vEdge.

```
log:local7.debug: May 7 16:58:19 vedge2 TTMD[683]: ttm_debug_announcement[194]: Received TTM Msg LINK_BFD, Client: ftmd, AF: LINK log:loc
```

تأكد من تشغيل `debug ttm events` على vEdge لتتبع Tunnel Traffic Manager (TTM) عند بدء تشغيل vEdge.

- [Cisco Systems - تادنتس مل اوى نة بتلا م عدلا](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا ة ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا