أستكشاف أخطاء شبكة VXLAN متعددة المواقع وإصلاحها باستخدام CloudSec في مخطط المربع

المحتويات

المقدمة

يصف هذا المستند تكوين المواقع المتعددة لشبكة VXLAN واستكشاف الأخطاء وإصلاحها باستخدام CloudSec بين بوابات الحدود المتصلة في مخطط مربع.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون على دراية بالمواضيع التالية:

- برنامج Nexus NXOS©.
- تقنية VXLAN EVPN.
- بروتوكولات توجيه BGP و OSPF.

المكونات المستخدمة

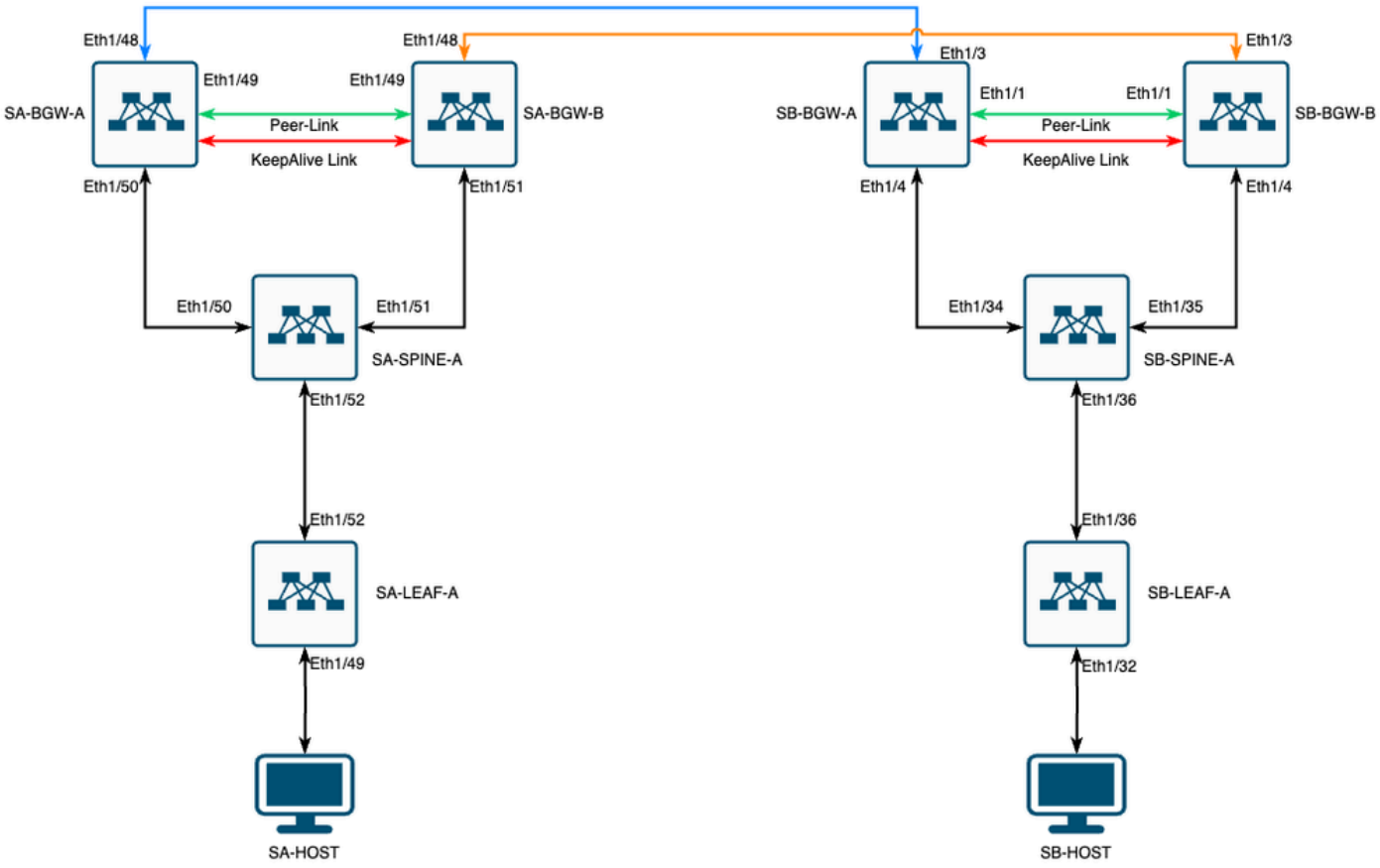
أستند المعلومة في هذا وثيقة على هذه برمجية وجهاز صيغة:

- Cisco Nexus 9000.
- NXOS الإصدار 10.3(4a).

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

الرسم التخطيطي للشبكة



VXLAN MultiSite مع CloudSec في طوبولوجيا مربعة

تفاصيل الطوبولوجيا

- نسيج شبكة EVPN متعدد المواقع للشبكة المحلية الظاهرية (VXLAN).
- تم تكوين كل المواقعين باستخدام بوابات حدود vPC.
- تتم إستضافة نقاط النهاية في شبكة VLAN 1100.
- تتضمن البوابات الحدودية على كل موقع منطقة جوار IPv4 iBGP بين بعضها البعض عبر شبكة VLAN3600 الخاصة بواجهة SVI.
- تتضمن البوابات الحدودية في أحد المواقع منطقة جوار eBGP IPv4 فقط مع بوابة الحدود المتصلة مباشرة في الموقع الآخر.
- تتضمن بوابات الحدود في الموقع A جوار EVPN eBGP L2VPN مع بوابات الحدود في الموقع B.

خطة العنونة

يتم إستخدام عناوين IP في الجدول أثناء التكوين:

	الموقع أ	الموقع باء				
دور الجهاز	معرف الواجهة	Physical Int IP	RID Loop IP	NVE Loop IP	MSITE-VIP	النسخ الاحتياطي لبروتوكول SVI IP
عمود فقري	المعيار ETH1/52	192.168.1.1/30	192.168.2.1/32	192.168.3.1/32	غير متوفر	غير متوفر
	المعيار ETH1/52	192.168.1.2/30			غير متوفر	
المعيار ETH1/34	المعيار ETH1/50	192.168.1.5/30	192.168.2.2/32	غير متوفر	غير متوفر	غير متوفر
ETH1/35	المعيار ETH1/51	192.168.1.9/30		غير متوفر		
192.168.4.1	بي جي بي-بلوي-إيه	المعيار ETH1/51	192.168.1.6/30	192.168.2.3/32	192.168.3.2/32	192.168.100.1/32
ETH1/3	المعيار ETH1/48	10.12.10.1/30		192.168.3.254/32		
192.168.4.2	BGW-B	المعيار ETH1/51	192.168.1.10/30	192.168.2.4/32	192.168.3.3/32	192.168.100.1/32
ETH1/3	المعيار ETH1/48	10.12.10.5/30		192.168.3.254/32		

التكوينات

- لاحظ أنه في هذا الدليل يتم عرض التكوين المرتبط بالمواقع المتعددة فقط. للتكوين الكامل، يمكنك إستخدام دليل الوثائق الرسمية لشبكة VXLAN Cisco Nexus 9000 Series NX-OS VXLAN، الإصدار 10.3(x)

لتمكين CloudSec، يجب تكوين dci-advertise-pip الأمر تحت عبارة الحد متعددة المواقع الخاصة ب EVPN:

SA-BGW-A و SA-BGW-B	SB-BGW-A و SB-BGW-B
evpn multisite border-gateway 65001 dci-advertise-pip	evpn multisite border-gateway 65002 dci-advertise-pip

تكوين BGP

هذا التكوين خاص بالموقع.

SA-BGW-A و SA-BGW-B	SB-BGW-A و SB-BGW-B
router bgp 65001 address-family ipv4 unicast maximum-paths 64 address-family l2vpn evpn maximum-paths 64 additional-paths send additional-paths receive	router bgp 65002 address-family ipv4 unicast maximum-paths 64 address-family l2vpn evpn maximum-paths 64 additional-paths send additional-paths receive

- يسمح الأمر **maximum-path** باستقبال مسارات EBGP متعددة لـ2VPN EVPN من المجاور.
- يرشد الأمر **additional-path** عملية BGP للإعلان عن أن الجهاز قادر على إرسال/استقبال مسارات إضافية

لكل L3VNI VRFs على بوابات الحدود، يجب تكوين متعدد المسارات أيضا:

SA-BGW-A و SA-BGW-B	SB-BGW-A و SB-BGW-B
router bgp 65001 vrf tenant-1 address-family ipv4 unicast maximum-paths 64 address-family ipv6 unicast maximum-paths 64	router bgp 65002 vrf tenant-1 address-family ipv4 unicast maximum-paths 64 address-family ipv6 unicast maximum-paths 64

تكوين تشفير النفق

يجب أن يكون هذا التكوين هو نفسه على جميع بوابات الحدود:

key chain CloudSec_Key_Chain1 tunnel-encryption key 1000 key-octet-string Cl0udSec! cryptographic-algorithm AES_128_CMAC feature tunnel-encryp

هذا التكوين خاص بالموقع. يجب تطبيق الأمرtunnel-encryption فقط على الواجهة التي لها evpn multisite dci-trackingأمر.

SA-BGW-A و SA-BGW-B	SB-BGW-A و SB-BGW-B
tunnel-encryption peer-ip 192.168.13.2 keychain CloudSec_Key_Chain1 policy CloudSec_Policy1 tunnel-encryption peer-ip 192.168.13.3 keychain CloudSec_Key_Chain1 policy CloudSec_Policy1 interface Ethernet1/48 tunnel-encryption	tunnel-encryption peer-ip 192.168.3.2 keychain CloudSec_Key_Chain1 policy CloudSec_Policy1 tunnel-encryption peer-ip 192.168.3.3 keychain CloudSec_Key_Chain1 policy CloudSec_Policy1 interface Ethernet1/3 tunnel-encryption

بعد تمكين ميزة تشفير النفق، تمت إضافة سمات إضافية إلى الاسترجاع المحلي أثناء إعلان المسارات إلى المجاور
ويجب أن ترى جميع جيران البث الأحادي eBGP IPv4 هذه السمة:

<#root>

SA-BGW-A# show ip bgp 192.168.2.3 BGP routing table information for VRF default, address family IPv4 Unicast BGP routing table entry for 192.168.2

!---

This is a new attribute

Path type: redist, path is valid, not best reason: Locally originated, no labeled nexthop AS-Path: NON

بالنسبة لنوع المسار-2، هناك أيضا سمة جديدة:

<#root>

SA-BGW-A# show bgp l2vpn evpn 00ea.bd27.86ef BGP routing table information for VRF default, address family L2VPN EVPN Route Distinguisher: 65

!---

Ethernet Segment Identifier (ESI) is also new attribute

Path-id 1 (dual) advertised to peers: 192.168.2.2 SA-BGW-A#

التحقق من الصحة

قبل تمكين CloudSec، من الجيد التحقق مما إذا كان الإعداد يعمل بشكل جيد بدون:

SA-BGW-A(config)# show clock Warning: No NTP peer/server configured. Time may be out of sync. 10:02:01.016 UTC Fri Jul 19 2024 Time source is N

بعد تكوين CloudSec أيضا، يجب أن تقوم نقطة النهاية على SA بنجاح بإختبار نقطة النهاية على الموقع B. ولكن في
بعض الحالات قد يكون إختبار الاتصال غير ناجح. يعتمد على أي ظير CloudSec تم تحديده بواسطة الجهاز المحلي للراسل
حركة مرور CloudSec المشفرة.

SA-HOST-A# ping 10.100.20.10 PING 10.100.20.10 (10.100.20.10): 56 data bytes Request 0 timed out Request 1 timed out Request 2 timed out Request 3

استكشاف الأخطاء وإصلاحها

تحقق من جدول ARP المحلي على نقطة نهاية المصدر:

SA-HOST-A# ping 10.100.20.10 count unlimited interval 1 Request 352 timed out Request 353 timed out Request 354 timed out 356 packets transmitted, (

يثبت هذا الإخراج أن، حركة مرور BUM تمر ومستوى التحكم يعمل. تتمثل الخطوة التالية في التحقق من حالة تشفير النفق:

SA-BGW-A# show tunnel-encryption session Tunnel-Encryption Peer Policy Keychain RxStatus TxStatus ----------------------- --------------------------------

يوضح هذا الإخراج أنه تم إنشاء جلسة عمل CloudSec. وكخطوة تالية، يمكنك تشغيل إختبار اتصال غير محدود على SA-Host-A:

SA-HOST-A# ping 10.100.20.10 count unlimited interval 1

من هذه النقطة يجب التحقق من الأجهزة الموجودة في الموقع A ومعرفة ما إذا كانت حركة مرور البيانات تصل إلى هذه الأجهزة. يمكنك إنجاز هذه المهمة باستخدام ELAM على جميع الأجهزة الموجودة على المسار في الموقع A. يسمح التغيير in-select من القيمة الافتراضية التي تتراوح بين 6 و 9 بالمطابقة استنادا إلى الرؤوس الداخلية. يمكنكم قراءة المزيد عن ELAM على هذا الرابط: [Nexus 9000 Cloud Scale ASIC (Tahoe) NX-OS ELAM.](#)

ELAM على SA-Leaf-A

في شبكة الإنتاج يوجد أكثر من جهاز رئيسي واحد. لكي تفهم العمود الفقري الذي أرسلت اليه حركة المرور، يجب ان تأخذ ELAM على الورقة اولا. على الرغم من أن in-select 9 يستعمل، في الورقة يربط إلى المصدر، ال خارجي IPv4 عنوان ينبغي تنت استعملت، بما أن الحركة مرور يبلغ هذا ورقة ال VXLAN يشفر. في الشبكة الحقيقية، من الممكن أن يكون من الصعب صيد الحزمة التي قمت بتوليدها بدقة. في مثل هذه الحالات، أنت يستطيع عيّركت تضخ عملية أزيز مع طول خاص واستعملت ال pkt len رأس أن يعين الربط ك. بشكل افتراضي، يبلغ طول حزمة ICMP 64 بايت. بالإضافة إلى 20 بايت من رأس IP، والذي منحك بشكل ملخص 84 بايت PKT Len:

<#root>

SA-LEAF-A# debug platform internal tah elam SA-LEAF-A(TAH-elam)# trigger init in-select 9 Slot 1: param values: start asic 0, start slice 0, lu-a2d 1, in

!---Note dpid value

```
 Dst Idx : 0xcd, Dst BD : 1100 Packet Type: IPv4 Outer Dst IPv4 address: 10.100.20.10 Outer Src IPv4 add
```

Pkt len = 84

```
, Checksum = 0xb4ae
```

!---64 byte + 20 byte IP header Pkt len = 84

```
 Inner Payload Type: CE L4 Protocol : 1 L4 info not available Drop Info: ---------- LUA: LUB: LUC: LUD:
```

!---

Put dpid value here

```
IF_STATIC_INFO: port_name=Ethernet1/52,if_index:0x1a006600,ltl=5940,slot=0, nxos_port=204,dmod=1,dpid=
```

من هذا الإخراج، يمكنك أن ترى حركة المرور يتم الوصول إليها من خلال SA-LEAF-A وإعادة توجيهها عبر الواجهة Ethernet1/52، المتصلة ب SA-SPINE-A من المخطط.

ELAM على جنوب العمود الفقري

على العامود الرئيسي، ال pkt len ستكون قيمة أكثر، بما أن ال 50 بايت VXLAN يضيف رأس أيضا. بشكل افتراضي، ال يمكن أن تتطابق العامود الرئيسي مع الرؤوس الداخلية بدون vxlan-parse أو feature nv overlay . لذلك، أنت ينبغي تستعمل vxlan-parse enable أمر على العامود الرئيسي:

<#root>

SA-SPINE-A(config-if)# debug platform internal tah elam SA-SPINE-A(TAH-elam)# trigger init in-select 9 Slot 1: param values: start asic 0, start slice 0,

!---

84 bytes + 50 bytes VXLAN header Pkt len = 134

```
Inner Payload Type: IPv4 Inner Dst IPv4 address: 10.100.20.10 Inner Src IPv4 address: 10.100.10.10 L4 
```

يرسل SA-SPINE-A حركة مرور باتجاه SA-BGW-A وفقا للإخراج.

ELAM على SA-BGW-A

SA-BGW-A(TAH-elam-insel9)# set inner ipv4 src_ip 10.100.10.10 dst_ip 10.100.20.10 SA-BGW-A(TAH-elam-insel9)# start SA-BGW-A(TAH-elam-ins

طبقا للناتج من SA-BGW-A، تم سحب حركة مرور البيانات من Ethernet1/48 باتجاه SB-BGW-A. والخطوة التالية هي فحص SB-BGW-A:

<#root>

SB-BGW-A# debug platform internal tah elam SB-BGW-A(TAH-elam)# trigger init in-select 9 Slot 1: param values: start asic 0, start slice 0, lu-a2d 1, in-

!---Reset the previous filter and start again just in case if packet was not captured.

```
SB-BGW-A(TAH-elam-insel9)# reset SB-BGW-A(TAH-elam-insel9)# set inner ipv4 src_ip 10.100.10.10 dst_ip 
```

ووفقا لمخرجات إس بي جي دبليو إيه، لم يتم إطلاق ELAM حتى. هذا يعني أنه إما أن SB-BGW-B يستلم الحزم ولا يكون قادرا على التعرف عليها بشكل صحيح، أو أنه لا يستلمها على الإطلاق. لفهم ما حدث مع حركة مرور CloudSec، يمكنك تشغيل ELAM على SB-BGW-A مرة أخرى، ولكن يجب تعيين عامل تصفية المشغل على عنوان IP الخارجي الذي يتم إستخدامه ل CloudSec، حيث ال توجد طريقة لرؤية الرأس الداخلي لحزمة النقل المشفرة ل CloudSec. من الإخراج السابق الذي تعرف، أن SA-BGW-A عالج حركة مرور البيانات، وهو ما يعني أن SA-BGW-A يشفر حركة مرور البيانات باستخدام CloudSEC.

لذلك، يمكنك استخدام NVE IP من SA-BGW-A كعامل تصفية مشغل ل ELAM. من الخارج الساقي، يبلغ طول حزمة ICMP
المشفرة ل VXLAN 134 بايت. يمكن رأس CloudSec بحجم 32 بايت في الملخص 166 بايت:

<#root>

SB-BGW-A(TAH-elam-insel9)# reset SB-BGW-A(TAH-elam-insel9)# set outer ipv4 src_ip 192.168.3.2 SB-BGW-A(TAH-elam-insel9)# start SB-BGW-A

192.168.13.3 *!---NVE IP address of SB-BGW-B*

Outer Src IPv4 address: 192.168.3.2 Ver = 4, DSCP = 0, Don't Fragment = 0 Proto = 17, TTL = 254, More

!---134 byte VXLAN packet + 32 byte cloudsec header Pkt len = 166

Inner Payload Type: CE L4 Protocol : 17 L4 info not available Drop Info: ---------- LUA: LUB: LUC: LUD

!---To reach SB-BGW-B NVE IP traffic was sent out of Ethernet1/4 which is connected to SB-SPINE-A

SB-BGW-A(TAH-elam-insel9)# show system internal ethpm info all | i i "dpid=130" IF_STATIC_INFO: port_n
SB-BGW-A(TAH-elam-insel9)# show cdp neighbors interface ethernet 1/4 Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge S - S

192.168.13.3/32

, ubest/mbest: 1/0 *via 192.168.11.5,

Eth1/4

, [110/6], 00:56:13, ospf-UNDERLAY, intra via

192.168.14.2

, [200/0], 01:13:46, bgp-65002, internal, tag 65002

!---The device still have a route for SB-BGW-B NVE IP via SVI

SB-BGW-A(TAH-elam-insel9)# show ip route 192.168.14.2 IP Route Table for VRF "default" '*' denotes best

***via 192.168.14.2, Vlan3600**

, [250/0], 01:15:05, am SB-BGW-A(TAH-elam-insel9)# show ip arp 192.168.14.2 Flags: * - Adjacencies lear

ecce.1324.c803

Vlan3600

SB-BGW-A(TAH-elam-insel9)# show mac address-table address ecce.1324.c803 Legend: * - primary entry, G

3600

ecce.1324.c803

static - F F

vPC Peer-Link(R)

SB-BGW-A(TAH-elam-insel9)#

من اذه الإخراج، يمكنك أن ترى، أن حركة مرور CloudSec تمت إعادة توجيهها نحو SB-BGW-B عبر واجهة إيثرنت 1/4، استنادا إلى
جدول التوجيه. وفقا لدليل تكوين شبكة NX-OS VXLAN من Cisco Nexus 9000 Series، الإصدار 10.3(x) من الإرشادات والقيود:

-

يجب أن تدخل حركة مرور CloudSec الموجهة للمحول المحول من خلال وصلات DCI.

ينطبق قسم معد عبارة الحدود vPC ل Cloudsec من نفس الدليل، إذا تعلم BGW من vPC عنوان PIP للنظير vPC BGWs والإعلان عن ذلك على جانب DCI، فإن سمات مسار BGP من كل من vPC BGW ستكون متطابقة. وبالتالي يمكن أن ينتهي الأمر بعقد DCI الوسيطة باختيار المسار من vPC BGW الذي لا يملك عنوان PIP. في هذا السيناريو، يتم استخدام ارتباط MCT لحركة المرور المشفرة القادمة من الموقع البعيد. ولكن في هذه الحالة، يتم استخدام الواجهة باتجاه العامود الرئيسي، برغم ذلك، فإن BGWs لديها أيضا تجاور OSPF عن طريق SVI الخلفي.

SB-BGW-A(TAH-elam-insel9)# show ip ospf neighbors OSPF Process ID UNDERLAY VRF default Total number of neighbors: 2 Neighbor ID Pri State

سبب المشكلة وإصلاحها

السبب هو تكلفة OSPF لواجهة SVI. بشكل افتراضي، يكون النطاق الترددي المرجعي للتكلفة التلقائية ل NXOS هو 40G. تحتوي واجهات SVI على نطاق ترددي عريض بسرعة 1 جيجابت في الثانية، بينما تحتوي الواجهة المادية على نطاق ترددي عريض بسرعة 10 جيجابت في الثانية:

<#root>

SB-BGW-A(TAH-elam-insel9)# show ip ospf interface brief OSPF Process ID UNDERLAY VRF default Total number of interface: 5 Interface ID Area C

<Output omitted>

```
 Eth1/4 5 0.0.0.0 1 P2P 1 up
```

في مثل هذه الحالة، التغيير الإداري لتكلفة SVI يستطيع حل الإصدار. يجب إجراء التوليف على جميع بوابات الحدود.

<#root>

SB-BGW-A(config)# int vlan 3600 SB-BGW-A(config-if)# ip ospf cost 1 SB-BGW-A(config-if)# sh ip route 192.168.13.3 IP Route Table for VRF "defau

via 192.168.14.2

```
, Vlan3600, [110/2], 00:00:08, ospf-UNDERLAY, intra via 192.168.14.2, [200/0], 01:34:07, bgp-65002, int
```

!---The ping is started to work immediately

Request 1204 timed out Request 1205 timed out Request 1206 timed out 64 bytes from 10.100.20.10: icmp_seq=1207 ttl=254 time=1.476 ms 64 bytes fron

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).