الترحيل السريع لتكوين نفق IKEv1 إلى IKEv2 L2L على رمز ASA 8.4

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاصطلاحات
لماذا الترحيل إلى IKEv2؟
نظرة عامة على الترحيل
عملية الهجرة
التكوين
التحقق من إنشاء نفق IKEv2
التحقق من PSK بعد الترحيل
عملية IKEv2 ومدير النفق
الآلية الاحتياطية لـ IKEv2 إلى IKEv1
هاردن IKEv2
معلومات ذات صلة

المقدمة

يوفر هذا المستند معلومات حول IKEv2 وعملية الترحيل من IKEv1.

المتطلبات الأساسية

المتطلبات

تأكد من وجود جهاز أمان Cisco ASA الذي يشغل IPsec باستخدام طريقة مصادقة مفتاح IKEv1 المشترك مسبقا (PSK)، وتأكد من أن نفق IPsec في حالة التشغيل.

على سبيل المثال، تكوين جهاز أمان Cisco ASA الذي يشغل IPsec باستخدام طريقة مصادقة IKEv1 PSK، ارجع إلى PIX/ASA 7.x وأعلى: مثال تكوين نفق PIX-to-PIX VPN.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات المكونات المادية والبرامج التالية.

- جهاز الأمان Cisco ASA 5510 Series Security Appliance الذي يعمل باستخدام الإصدار x.8.4 والإصدارات الأحدث.

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

الاصطلاحات

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى اصطلاحات تلميحات Cisco التقنية.

لماذا الترحيل إلى IKEv2؟

- يوفر IKEv2 مرونة هجوم الشبكة بشكل أفضل. يمكن أن يخفف IKEv2 هجوم رفض الخدمة (DoS) على الشبكة عند التحقق من صحة بادئ IPsec. ولجعل قابلية تعرض "رفض الخدمة" صعبة الاستغلال، يمكن للمستجيب أن يطلب ملف تعريف إرتباط إلى البادئ الذي عليه أن يضمن للمسؤول أن هذا اتصال عادي. في IKEv2، تخفف ملفات تعريف الارتباط الخاصة بالمستجيب من هجوم رفض الخدمة (DoS) بحيث لا يحتفظ المستجيب بحالة بادئ IKE أو لا يقوم بعملية D-H ما لم يرجع البادئ ملف تعريف الارتباط الذي أرسله المستجيب. يستخدم المستجيب الحد الأدنى من وحدة المعالجة المركزية (CPU) ولا يلزم أي دولة باقتران الأمان (SA) حتى يتمكن من التحقق من صحة البادئ بشكل كامل.
- يعمل IKEv2 على تقليل التعقيد في إنشاء IPsec بين منتجات الشبكات الخاصة الظاهرية (VPN) المختلفة. كما أنه يزيد من إمكانية التشغيل البيني ويتيح طريقة قياسية لطرق المصادقة القديمة. يوفر IKEv2 قابلية التشغيل البيني بسلاسة عبر بروتوكول IPsec بين الموردين نظرا لأنه يوفر تقنيات مدمجة مثل اكتشاف النظير الميت (DPD) أو إجتياز NAT (NAT-T) أو الاتصال الأولي.
- يحتوي IKEv2 على مصروفات عامة أقل. وبفضل التكاليف الإضافية الأقل، يوفر هذا الطراز زمن وصول محسن لإعداد SA. يتم السماح بطلبات متعددة أثناء النقل (على سبيل المثال، عندما يتم إعداد عدة شبكات فرعية في نفس الوقت).
- يحتوي IKEv2 على تأخر SA مخفض. في IKEv1 يضخم تأخير إنشاء SA مع تضخيم حجم الحزمة. يحتفظ IKEv2 بنفس معدل التأخير عند تضخيم حجم الحزمة. عندما يتم تضخيم حجم الحزمة، يتم تضخيم وقت تشفير رأس الحزمة ومعالجته. عندما يتم إنشاء مؤسسة SA جديدة، يلزم المزيد من الوقت. قيمة SA التي تم إنشاؤها بواسطة IKEv2 أقل من تلك التي تم إنشاؤها بواسطة IKEv1. بالنسبة لحجم الحزمة المكبر، فإن الوقت المستغرق لإنشاء SA ثابت تقريبا.
- يتمتع IKEv2 بوقت إعادة توجيه أسرع. يستغرق IKE v1 وقتا أطول لإعادة تكوين SAs من IKEv2. يوفر IKEv2 rekey ل SA أداء أمان محسنا ويقلل عدد الحزم المفقودة في المرحلة الانتقالية. نظرا لإعادة تعريف بعض آليات IKEv1 (مثل حمولة ToS واختيار عمر SA وتفرد SPI) في IKEv2، يتم فقد عدد أقل من الحزم وتكرارها في IKEv2. وبالتالي، هناك حاجة أقل إلى إصلاح إتفاقات الخدمة الخاصة.

ملاحظة: نظرا لأن أمان الشبكة لا يمكن أن يكون قويا إلا بقدر أضعف إرتباط، فإن IKEv2 لا يعمل مع IKEv1.

نظرة عامة على الترحيل

إذا كان التكوين الخاص بك IKEv1 أو حتى SSL موجودا بالفعل، فإن ASA يجعل عملية الترحيل بسيطة. في سطر الأوامر، أدخل الأمر **migrate**:

```
{migrate {l2l | remote-access {ikev2 | ssl} | overwrite
```

أشياء جديرة بالملاحظة:

- تعريفات الكلمات الأساسية:**L2l** - يحول هذا أنفاق IKEv1 l2l الحالية إلى IKEv2.**الوصول عن بعد** - يؤدي ذلك إلى تحويل تكوين الوصول عن بعد. يمكنك تحويل إما IKEv1 أو مجموعات نفق SSL إلى IKEv2.**overwrite** - إذا كان لديك تكوين IKEv2 ترغب في الكتابة فوقه، فعندئذ تقوم هذه الكلمة الأساسية بتحويل تكوين IKEv1

الحالي وإزالة تكوين IKEv2 غير الهام.

- من المهم ملاحظة أن IKEv2 لديه القدرة على إستخدام كل من المفاتيح المتماثلة وغير المتماثلة لمصادقة PSK. عند إدخال الأمر **migration** على ASA، يقوم ASA تلقائيا بإنشاء IKEv2 VPN باستخدام PSK متماثل.
- بعد إدخال الأمر، لا يتم حذف تكوينات IKEv1 الحالية. وبدلا من ذلك، يتم تشغيل كل من تكوينات IKEv1 و IKEv2 بالتوازي وعلى خريطة التشفير نفسها. يمكنك فعل ذلك يدويا أيضا. عند تشغيل كل من IKEv1 و IKEv2 بشكل متواز، يسمح ذلك لبادئ VPN ل IPsec بإجراء عمليات النسخ الاحتياطي من IKEv2 إلى IKEv1 عند وجود بروتوكول أو مشكلة تكوين مع IKEv2 يمكن أن تؤدي إلى فشل محاولة الاتصال. عند تشغيل كل من IKEv1 و IKEv2 بالتوازي، فإنه يوفر أيضا آلية التراجع ويجعل الترحيل أسهل.
- عند تشغيل كل من IKEv1 و IKEv2 بالتوازي، يستخدم ASA وحدة نمطية تسمى مدير النفق/IKE المشترك في البادئ لتحديد خريطة التشفير وإصدار بروتوكول IKE للاستخدام مع الاتصال. ودائما ما يفضل ASA بدء تشغيل IKEv2، ولكن إذا تعذر ذلك، فإنه يرجع إلى IKEv1.
- لا يتم دعم الأقران المتعددة المستخدمة للتكرار مع IKEv2 على ASA. في IKEv1، ولأغراض التكرار، يمكن أن يكون للمرء أكثر من نظير واحد ضمن خريطة التشفير نفسها عند إدخال أمر **تعيين النظير**. سيكون النظير الأول هو الأساسي وإذا فشل، فسيبدأ النظير الثاني في العمل. أحلت cisco بق CSCud2276 id (سجل زبون فقط)، enh: يتعدد نظير دعم ل IKEv2.

عملية الهجرة

التكوين

في هذا المثال، توجد IKEv1 VPN التي تستخدم مصادقة المفتاح المشترك مسبقا (PSK) على ASA.

ملاحظة: التكوين الظاهر هنا وثيق الصلة فقط بنفق VPN.

تكوين ASA باستخدام شبكة VPN الحالية ل IKEv1 (قبل الترحيل)

```
ASA-2(config)# sh run
(ASA Version 8.4(2
!
hostname ASA-2
!
crypto ipsec IKEv1 transform-set goset esp-3des esp-sha-hmac
crypto map vpn 12 match address NEWARK
crypto map vpn 12 set pfs group5
<crypto map vpn 12 set peer <peer_ip-address
crypto map vpn 12 set IKEv1 transform-set goset
crypto map vpn interface outside
crypto isakmp disconnect-notify
crypto IKEv1 enable outside
crypto IKEv1 policy 1
authentication pre-share
encryption 3des
hash sha
group 5
lifetime 86400
!
tunnel-group <peer_ip-address> type ipsec-l2l
tunnel-group <peer_ip-address> ipsec-attributes
***** IKEv1 pre-shared-key
isakmp keepalive threshold 10 retry 3
```

تكوين ASA IKEv2 (بعد الترحيل)

ملاحظة: التغييرات التي تم وضع علامة عليها بالخط المائل الغامق.

```
ASA-2(config)# migrate l2l
ASA-2(config)# sh run
(ASA Version 8.4(2
!
hostname ASA-2
!
crypto ipsec IKEv1 transform-set goset esp-3des esp-sha-hmac

crypto ipsec IKEv2 ipsec-proposal goset protocol esp encryption 3des protocol esp integrity sha-1
crypto map vpn 12 match address NEWARK
crypto map vpn 12 set pfs group5
<crypto map vpn 12 set peer <peer_ip-address
crypto map vpn 12 set IKEv1 transform-set goset

crypto map vpn 12 set IKEv2 ipsec-proposal goset
crypto map vpn interface outside
crypto isakmp disconnect-notify

crypto IKEv2 policy 1 encryption 3des integrity sha group 5 prf sha lifetime seconds 86400
crypto IKEv2 enable outside
crypto IKEv1 enable outside
crypto IKEv1 policy 1
authentication pre-share
encryption 3des
hash sha
group 5
lifetime 86400
!
tunnel-group <peer_ip-address> type ipsec-l2l
tunnel-group <peer_ip-address> ipsec-attributes
***** IKEv1 pre-shared-key
isakmp keepalive threshold 10 retry 3

***** IKEv2 remote-authentication pre-shared-key ***** IKEv2 local-authentication pre-shared-key
```

التحقق من إنشاء نفق IKEv2

```
ASA1# sh cry IKEv2 sa detail

:IKEv2 SAs
Session-id:12, Status:UP-ACTIVE, IKE count:1, CHILD count:1
Tunnel-id   Local                Remote     Status        Role
READY    INITIATOR  192.168.2.2/500  192.168.1.1/500 102061223
Encr: 3DES, Hash: SHA96, DH Grp:5, Auth sign: PSK,Auth verify: PSK
Life/Active Time: 86400/100 sec
Status Description: Negotiation done
Local spi: 297EF9CA996102A6       Remote spi: 47088C8FB9F039AD
Local id: 192.168.1.1
Remote id: 192.168.2.2
DPD configured for 10 seconds, retry 3
NAT-T is not detected
Child sa: local selector  10.10.10.0/0 - 10.10.10.255/65535
remote selector 10.20.20.0/0 - 10.20.20.255/65535
ESP spi in/out: 0x637df131/0xb7224866

ASA1# sh crypto ipsec sa
```

```
                                                interface: outside
                                Crypto map tag: vpn, seq num: 12, local addr: 192.168.1.1
                    access-list NEWARK extended permit ip 10.10.10.0 255.255.255.0
                                                        255.255.255.0 10.20.20.0
                  (local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0
                 (remote ident (addr/mask/prot/port): (10.20.20.0/255.255.255.0/0/0
                                                        current_peer: 192.168.2.2
                                    pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4#
```

التحقق من PSK بعد الترحيل

للتحقق من PSK، يمكنك تشغيل هذا الأمر في وضع التكوين العام:

```
more system: running-config | beg tunnel-group
```

عملية IKEv2 ومدير النفق

وكما تمت الإشارة مسبقا، يستخدم ASA وحدة نمطية تسمى مدير النفق/IKE المشترك في البادئ لتحديد خريطة التشفير وإصدار بروتوكول IKE للاستخدام مع الاتصال. دخلت هذا أمر أن يراقب الوحدة نمطية:

```
<debug crypto ike-common <level
```

تم تجميع أوامر **تصحيح الأخطاء** و**logging** و**show** عند تمرير حركة مرور البيانات لبدء نفق IKEv2. للوضوح، تم حذف بعض المخرجات.

```
                                                ASA1(config)# logging enable
                                ASA1(config)# logging list IKEv2 message 750000-752999
                                                ASA1(config)# logging console IKEv2
                                                        ASA1(config)# exit
                                                ASA1# debug crypto IKEv2 platform 4
                                                ASA1# debug crypto IKEv2 protocol  4
                                                    ASA1# debug crypto ike-common 5

                .ASA-5-752003: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv2%
                                                        .Map Tag = vpn.  Map Sequence Number = 12
            ASA-5-750001: Local:192.168.1.1:500 Remote:192.168.2.2:500 Username:Unknown%
:Received request to establish an IPsec tunnel; local traffic selector = Address Range
                                                Protocol: 0 10.10.10.11-10.10.10.11
                                :Port Range: 0-65535; remote traffic selector = Address Range
                                    Protocol: 0 Port Range: 0-65535 10.20.20.21-10.20.20.21
              Mar 22 15:03:52 [IKE COMMON DEBUG]Tunnel Manager dispatching a KEY_ACQUIRE
                                .message to IKEv2.  Map Tag = vpn.  Map Sequence Number = 12
                        IKEv2-PLAT-3: attempting to find tunnel group for IP: 192.168.2.2
                           IKEv2-PLAT-3: mapped to tunnel group 192.168.2.2 using peer IP
                        26%ASA-5-750006: Local:192.168.1.1:500 Remote:192.168.2.2:500
                           Username:192.168.2.2 SA UP. Reason: New Connection Established
                            .43%ASA-5-752016: IKEv2 was successful at setting up a tunnel
                                                .Map Tag = vpn. Map Sequence Number = 12
                            .ASA-7-752002: Tunnel Manager Removed entry.  Map Tag = vpn%
                                                        .Map Sequence Number = 12
                    IKEv2-PLAT-4: SENT PKT [IKE_SA_INIT] [192.168.1.1]:500->[192.168.2.2]:500
                           InitSPI=0x297ef9ca996102a6 RespSPI=0x0000000000000000 MID=00000000
                                                    IKEv2-PROTO-3: (12): Insert SA
                    IKEv2-PLAT-4: RECV PKT [IKE_SA_INIT] [192.168.2.2]:500->[192.168.1.1]:500
                           InitSPI=0x297ef9ca996102a6 RespSPI=0x47088c8fb9f039ad MID=00000000
                       IKEv2-PLAT-4: SENT PKT [IKE_AUTH] [192.168.1.1]:500->[192.168.2.2]:500
                           InitSPI=0x297ef9ca996102a6 RespSPI=0x47088c8fb9f039ad MID=00000001
                       IKEv2-PLAT-4: RECV PKT [IKE_AUTH] [192.168.2.2]:500->[192.168.1.1]:500
                           InitSPI=0x297ef9ca996102a6 RespSPI=0x47088c8fb9f039ad MID=00000001
```

```
IKEv2-PROTO-3: (12): Verify peer's policy
IKEv2-PROTO-3: (12): Get peer authentication method
IKEv2-PROTO-3: (12): Get peer's preshared key for 192.168.2.2
IKEv2-PROTO-3: (12): Verify authentication data
IKEv2-PROTO-3: (12): Use preshared key for id 192.168.2.2, key len 5
IKEv2-PROTO-2: (12): SA created; inserting SA into database
:IKEv2-PLAT-3
CONNECTION STATUS: UP... peer: 192.168.2.2:500, phase1_id: 192.168.2.2
IKEv2-PROTO-3: (12): Initializing DPD, configured for 10 seconds
IKEv2-PLAT-3: (12) DPD Max Time will be: 10
IKEv2-PROTO-3: (12): Checking for duplicate SA
.Mar 22 15:03:52 [IKE COMMON DEBUG]IKEv2 was successful at setting up a tunnel
.Map Tag = vpn. Map Sequence Number = 12
.Mar 22 15:03:52 [IKE COMMON DEBUG]Tunnel Manager Removed entry
.Map Tag = vpn.  Map Sequence Number = 12
```

الآلية الاحتياطية ل IKEv2 إلى IKEv1

ومع وجود كل من IKEv1 و IKEv2 في نفس الوقت، يفضل مكتب المحاسبة على الدوام بدء تشغيل IKEv2. وإذا تعذر ذلك على ASA، فإنه يرجع إلى IKEv1. تقوم الوحدة النمطية المشتركة لمدير النفق/IKE بإدارة هذه العملية. في هذا المثال على البادئ، تم مسح IKEv2 SA وأصبح IKEv2 الآن مكونا بشكل غير متعمد (تم إزالة اقتراح IKEv2) لتوضيح آلية التراجع.

```
ASA1# clear  crypto  IKEv2 sa

ASA-5-750007: Local:192.168.1.1:500 Remote:192.168.2.2:500%
Username:192.168.2.2 SA DOWN. Reason: operator request
ASA1(config)# no crypto map vpn 12 set IKEv2 ipsec-proposal GOSET
ASA1# (config ) logging enable
ASA1# (config ) logging list IKEv2 message 750000-752999
ASA1# (config ) logging console IKEv2
ASA1# (config ) exit
ASA1# debug crypto IKEv2 platform 4
ASA1# debug crypto IKEv2 protocol  4
ASA1# debug crypto ike-common 5
.ASA-5-752004: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv1%
.Map Tag = vpn.  Map Sequence Number = 12
ASA-4-752010: IKEv2 Doesn't have a proposal specified%
Mar 22 15:11:44 [IKE COMMON DEBUG]Tunnel Manager dispatching a KEY_ACQUIRE
.message to IKEv1.  Map Tag = vpn.  Map Sequence Number = 12
Mar 22 15:11:44 [IKE COMMON DEBUG]IKEv2 Doesn't have a proposal specified
.ASA-5-752016: IKEv1 was successful at setting up a tunnel.  Map Tag = vpn%
.Map Sequence Number = 12
.ASA-7-752002: Tunnel Manager Removed entry.  Map Tag = vpn%
.Map Sequence Number = 12
.Mar 22 15:11:44 [IKE COMMON DEBUG]IKEv1 was successful at setting up a tunnel
.Map Tag = vpn. Map Sequence Number = 12
.Mar 22 15:11:44 [IKE COMMON DEBUG]Tunnel Manager Removed entry.  Map Tag = vpn
.Map Sequence Number = 12

ASA1(config)# sh cry IKEv2 sa
There are no IKEv2 SAs
ASA1(config)# sh cry IKEv1 sa
:IKEv1 SAs
Active SA: 1
(Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey
Total IKE SA: 1
IKE Peer: 192.168.2.2   1
Type    : L2L             Role    : initiator
Rekey   : no              State   : MM_ACTIVE
```

هاردن IKEv2

لتوفير أمان إضافي عند إستخدام IKEv2، يوصى بشدة باستخدام الأوامر الاختيارية التالية:

- **crypto IKEv2 cookie-challenge**: يمكن ASA من إرسال تحديات ملف تعريف الارتباط إلى الأجهزة النظيرة إستجابة للحزم التي تم بدء تشغيل SA نصفها.
- **crypto IKEv2 limit max-sa**: يحد عدد إتصالات IKEv2 على ASA. بشكل افتراضي، يساوي الحد الأقصى المسموح به لاتصال IKEv2 الحد الأقصى لعدد الاتصالات المحددة بواسطة ترخيص ASA.
- **التشفير IKEv2 الحد الأقصى للإدخال في التفاوض-sa**: تحديد عدد شبكات SA أثناء التفاوض (المفتوحة) ل IKEv2 على ASA. عند الاستخدام بالاقتران مع أمر **crypto IKEv2 cookie-challenge**، تأكد من أن عتبة تحدي ملفات تعريف الارتباط أقل من هذا الحد.

إستخدام مفاتيح غير متماثلة. بعد الترحيل، يمكن تعديل التكوين لاستخدام مفاتيح غير متماثلة كما هو موضح هنا:

```
ASA-2(config)# more system:running-config
tunnel-group <peer_ip-address> type ipsec-l2l
tunnel-group <peer_ip-address> ipsec-attributes
 IKEv1 pre-shared-key cisco1234
IKEv2 remote-authentication pre-shared-key cisco1234
IKEv2 local-authentication pre-shared-key cisco123
```

من المهم إدراك أنه يجب نسخ التكوين على النظير الآخر للمفتاح المشترك مسبقا IKEv2. لن يعمل إذا قمت بتحديد التكوين ولصقه من جانب إلى آخر.

ملاحظة: يتم تعطيل هذه الأوامر بشكل افتراضي.

معلومات ذات صلة

- الدعم التقني والمستندات

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).