تكوين نفق من موجه إلى موجه من شبكة LAN إلى شبكة LAN باستخدام موجه يقوم بتشغيل IKE الوضع العدواني

المحتويات

المقدمة

يقدم برنامج Cisco IOS® الإصدار 12.2(8)T وظائف الموجه لبدء تبادل مفتاح الإنترنت (IKE) في الوضع العدواني. لمزيد من المعلومات، راجع معرف الخطأ CSCdt30808 (العملاء المسجلون فقط) في مجموعة أدوات الخطأ. في السابق، كان الموجه قادرا على الاستجابة لطلب تفاوض نفق لوضع عدواني، ولكنه لم يكن قادرا أبدا على بدء تشغيله.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات أساسية خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية أدناه.

- تم إستخدام Cisco IOS 12.2(8)T على كلا الموجهين، رغم أنه ليس من الضروري وجوده على الموجه المستقبل.

ملاحظة: تم إختبار هذا التكوين باستخدام البرنامج Cisco IOS Software، الإصدار T1(13)12.2. تبقى جميع نواحي التكوين كما هي.

تم إنشاء المعلومات المُقدمة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كنت تعمل في شبكة مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر قبل استخدامه.

الاصطلاحات

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

معلومات أساسية

ملاحظة: أوامر واجهة سطر الأوامر (CLI) الجديدة هي كما يلي:

- **نظير التشفير </عنوان <*x.x.x.x*> | اسم المضيف <*name*> >**
- **<set aggressive-mode client-endpoint < fqdn <*name*> عنوان | user-fqdn <*name*> | IPv4 <*x.x.x*> <**
- **ضبط كلمة مرور الوضع العدائي <*password*>**

في نموذج التكوين أدناه، يحتوي الموجه A و RouterB على نفق من شبكة LAN بينهما. سيكون RouterA دائما هو النفق الذي يبدأ الموجه، وقد تم تكوينه في هذا المثال للبدء في وضع عدواني. يحتوي الموجه B ببساطة على خريطة تشفير ديناميكية لقبول معلمات النفق من RouterA، رغم أنه قد يكون قد تم تطبيق تكوين نفق من شبكة LAN إلى شبكة LAN قياسي.

ملاحظة: في هذا المثال، لا يلزم أن يقوم الموجه B بتشغيل الإصدار T(8)12.2 من برنامج Cisco IOS Software لقبول معلمات النفق من الموجه A. مثلما تمت الإشارة إليه أعلاه، كانت الموجهات تقبل دائما طلب وضع عدواني، ولكنها لم تكن قادرة أبدا على بدء تشغيله.

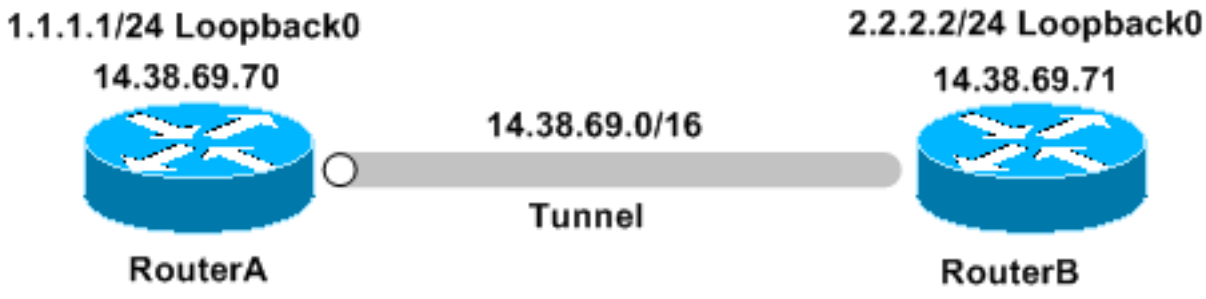
التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: للعثور على معلومات إضافية حول الأوامر المستخدمة في هذا المستند، أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط).

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة الموضح في الرسم التخطيطي أدناه.



التكوينات

يستخدم هذا المستند التكوينات التالية:

- الموجه A
- الموجه B

الموجه A

```
...Building configuration

Current configuration : 1253 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterA
!
!
memory-size iomem 10
ip subnet-zero
!
!
!
!
crypto isakmp policy 1
hash md5
authentication pre-share
crypto isakmp keepalive 30 5
!
crypto isakmp peer address 14.38.69.71
set aggressive-mode password cisco123
set aggressive-mode client-endpoint ipv4-address
14.38.69.70
!
!
crypto ipsec transform-set myset esp-3des esp-md5-hmac
!
crypto map mymap 1 ipsec-isakmp
set peer 14.38.69.71
set transform-set myset
match address 100
!
!
!
interface Loopback0
ip address 1.1.1.1 255.255.255.0
!
interface Ethernet0/0
ip address 14.38.69.70 255.255.0.0
half-duplex
crypto map mymap
!
interface BRI0/0
no ip address
shutdown
!
interface Ethernet0/1
no ip address
shutdown
half-duplex
```

```
!
ip classless
ip route 0.0.0.0 0.0.0.0 14.38.69.71
ip http server
!
!
access-list 100 permit ip 1.1.1.0 0.0.0.255 2.2.2.0
0.0.0.255
!
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
!
end
```

الموجه B

```
...Building configuration

Current configuration : 1147 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterB
!
!
ip subnet-zero
!
!
!
!
crypto isakmp policy 1
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 14.38.69.70
crypto isakmp keepalive 30 5
!
!
crypto ipsec transform-set myset esp-3des esp-md5-hmac
!
crypto dynamic-map mymap 10
 set transform-set myset
!
!
crypto map mainmap 1 ipsec-isakmp dynamic mymap
!
!
!
interface Loopback0
```

```
 ip address 2.2.2.2 255.255.255.0
 !
interface FastEthernet0/0
ip address 14.38.69.71 255.255.0.0
 duplex auto
 speed auto
crypto map mainmap
 !
interface Serial0/0
 no ip address
 shutdown
 no fair-queue
 !
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
 !
 ip classless
ip route 0.0.0.0 0.0.0.0 14.38.69.70
 no ip http server
 !
 !
 call rsvp-sync
 !
 !
mgcp profile default
 !
dial-peer cor custom
 !
 !
 line con 0
 exec-timeout 0 0
 speed 115200
 line aux 0
 line vty 0 4
 login
 !
 !
end
```

التحقق من الصحة

يوفر هذا القسم معلومات يمكنك إستخدامها للتأكد من أن التكوين يعمل بشكل صحيح.

يتم دعم بعض أوامر **العرض بواسطة** أداة مترجم الإخراج (العملاء المسجلون فقط)، والتي تتيح لك عرض تحليل إخراج أمر **العرض**.

- **show crypto ips sa**—يعرض اقترانات أمان المرحلة 2.
- **show crypto isakmp sa**—يعرض اقترانات أمان المرحلة 1

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

أوامر استكشاف الأخطاء وإصلاحها

ملاحظة: قبل إصدار أوامر **تصحيح الأخطاء**، يرجى الاطلاع على المعلومات المهمة في أوامر تصحيح الأخطاء.

- **debug crypto ipSec**—يعرض مفاوضات IPSec للمرحلة 2.
- **debug crypto isakmp**—يعرض مفاوضات ISAKMP للمرحلة 1.
- **debug crypto engine**—يعرض حركة مرور البيانات التي يتم تشفيرها.

إخراج تصحيح أخطاء الموجه A

```
, :(IPSEC(sa_request :00:08:26
,key eng. msg.) OUTBOUND local= 14.38.69.70, remote= 14.38.69.71)
,(local_proxy= 1.1.1.0/255.255.255.0/0/0 (type=4
,(remote_proxy= 2.2.2.0/255.255.255.0/0/0 (type=4
, protocol= ESP, transform= esp-3des esp-md5-hmac
,lifedur= 3600s and 4608000kb
spi= 0x4B68058A(1265108362), conn_id= 0, keysize= 0, flags= 0x400C
(ISAKMP: received ke message (1/1 :00:08:26
ISAKMP: local port 500, remote port 500 :00:08:26
.ISAKMP (0:1): SA has tunnel attributes set :00:08:26
!ISAKMP (0:1): SA is doing unknown authentication :00:08:26
ISAKMP (1): ID payload :00:08:26
next-payload : 13
type : 1
protocol : 17
port : 500
length : 8
ISAKMP (1): Total payload length: 12 :00:08:26
ISAKMP (0:1): Input = IKE_MESG_FROM_IPSEC, IKE_SA_REQ_AM :00:08:26
Old State = IKE_READY New State = IKE_I_AM1

ISAKMP (0:1): beginning Aggressive Mode exchange :00:08:26
....ISAKMP (0:1): sending packet to 14.38.69.71 (I) AG_INIT_E.XCH :00:08:26
(Success rate is 0 percent (0/5
vpn-2611a1#
...ISAKMP (0:1): retransmitting phase 1 AG_INIT_EXCH :00:08:36
ISAKMP (0:1): incrementing error counter on sa: retransmit phase 1 :00:08:36
ISAKMP (0:1): retransmitting phase 1 AG_INIT_EXCH :00:08:36
ISAKMP (0:1): sending packet to 14.38.69.71 (I) AG_INIT_EXCH :00:08:36
ISAKMP (0:1): received packet from 14.38.69.71 (I) AG_INIT_EXCH :00:08:37
ISAKMP (0:1): processing SA payload. message ID = 0 :00:08:37
.ISAKMP (0:1): SA using tunnel password as pre-shared key :00:08:37
ISAKMP (0:1): Checking ISAKMP transform 1 against priority 1 policy :00:08:37
ISAKMP: encryption DES-CBC :00:08:37
ISAKMP: hash MD5 :00:08:37
ISAKMP: default group 1 :00:08:37
ISAKMP: auth pre-share :00:08:37
ISAKMP: life type in seconds :00:08:37
ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80 :00:08:37
ISAKMP (0:1): atts are acceptable. Next payload is 0 :00:08:37
ISAKMP (0:1): processing vendor id payload :00:08:37
ISAKMP (0:1): vendor ID is Unity :00:08:37
ISAKMP (0:1): processing vendor id payload :00:08:37
ISAKMP (0:1): vendor ID is DPD :00:08:37
ISAKMP (0:1): processing vendor id payload :00:08:37
!ISAKMP (0:1): speaking to another IOS box :00:08:37
ISAKMP (0:1): processing vendor id payload :00:08:37
ISAKMP (0:1): processing KE payload. message ID = 0 :00:08:37
ISAKMP (0:1): processing ID payload. message ID = 0 :00:08:37
ISAKMP (0:1): processing NONCE payload. message ID = 0 :00:08:37
.ISAKMP (0:1): SA using tunnel password as pre-shared key :00:08:37
ISAKMP (0:1): SKEYID state generated :00:08:37
```

```
ISAKMP (0:1): processing HASH payload. message ID = 0 :00:08:37
ISAKMP (0:1): SA has been authenticated with 14.38.69.71 :00:08:37
ISAKMP (0:1): IKE_DPD is enabled, initializing timers :00:08:37
ISAKMP: Locking DPD struct 0x82702444 :00:08:37
from crypto_ikmp_dpd_ike_init, count 1
ISAKMP (0:1): sending packet to 14.38.69.71 (I) QM_IDLE :00:08:37
ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH :00:08:37
Old State = IKE_I_AM1  New State = IKE_P1_COMPLETE

...IPSEC(key_engine): got a queue event :00:08:37
IPSec: Key engine got KEYENG_IKMP_MORE_SAS message :00:08:37
(ISAKMP: received ke message (6/1 :00:08:37
ISAKMP: received KEYENG_IKMP_MORE_SAS message :00:08:37
ISAKMP (0:1): sending packet to 14.38.69.71 (I) QM_IDLE :00:08:37
ISAKMP (0:1): purging node -1844394438 :00:08:37
.ISAKMP (0:1): Sending initial contact :00:08:37

ISAKMP (0:1): received packet from 14.38.69.71 (I) QM_IDLE :00:08:37
ISAKMP (0:1): processing HASH payload. message ID = 133381228 :00:08:37
ISAKMP (0:1): processing NOTIFY RESPONDER_LIFETIME protocol 1 :00:08:37
spi 0, message ID = 133381228, sa = 82701CDC
ISAKMP (0:1): processing responder lifetime :00:08:37
ISAKMP (0:1): deleting node 133381228 error :00:08:37
"FALSE reason "informational (in) state 1
ISAKMP (0:1): Input = IKE_MESG_FROM_PEER, IKE_INFO_NOTIFY :00:08:37
Old State = IKE_P1_COMPLETE  New State = IKE_P1_COMPLETE

.ISAKMP: quick mode timer expired :00:08:38
ISAKMP (0:1): src 14.38.69.70 dst 14.38.69.71 :00:08:38
ISAKMP (0:1): beginning Quick Mode exchange, M-ID of -1119238561 :00:08:38
ISAKMP (0:1): sending packet to 14.38.69.71 (I) QM_IDLE :00:08:38
,ISAKMP (0:1): Node -1119238561, Input = IKE_MESG_INTERNAL :00:08:38
IKE_INIT_QM Old State = IKE_QM_READY  New State = IKE_QM_I_QM1

ISAKMP (0:1): received packet from 14.38.69.71 (I) QM_IDLE :00:08:38
ISAKMP (0:1): processing HASH payload. message ID = -1119238561 :00:08:38
ISAKMP (0:1): processing SA payload. message ID = -1119238561 :00:08:38
ISAKMP (0:1): Checking IPSec proposal 1 :00:08:38
ISAKMP: transform 1, ESP_3DES :00:08:38
:ISAKMP:   attributes in transform :00:08:38
ISAKMP:      encaps is 1 :00:08:38
ISAKMP:      SA life type in seconds :00:08:38
ISAKMP:      SA life duration (basic) of 3600 :00:08:38
ISAKMP:      SA life type in kilobytes :00:08:38
ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0 :00:08:38
ISAKMP:      authenticator is HMAC-MD5 :00:08:38
.ISAKMP (0:1): atts are acceptable :00:08:38
,IPSEC(validate_proposal_request): proposal part #1 :00:08:38
,key eng. msg.) INBOUND local= 14.38.69.70, remote= 14.38.69.71)
,(local_proxy= 1.1.1.0/255.255.255.0/0/0 (type=4
,(remote_proxy= 2.2.2.0/255.255.255.0/0/0 (type=4
, protocol= ESP, transform= esp-3des esp-md5-hmac
,lifedur= 0s and 0kb
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
ISAKMP (0:1): processing NONCE payload. message ID = -1119238561 :00:08:38
ISAKMP (0:1): processing ID payload. message ID = -1119238561 :00:08:38
ISAKMP (0:1): processing ID payload. message ID = -1119238561 :00:08:38
ISAKMP (0:1): Creating IPSec SAs :00:08:38
inbound SA from 14.38.69.71 to 14.38.69.70         :00:08:38
(proxy 2.2.2.0 to 1.1.1.0)
has spi 0x4B68058A and conn_id 2000 and flags 4         :00:08:38
lifetime of 3600 seconds         :00:08:38
lifetime of 4608000 kilobytes         :00:08:38
outbound SA from 14.38.69.70 to 14.38.69.71         :00:08:38
```

```
                                        (proxy 1.1.1.0 to 2.2.2.0)
     has spi 1503230765 and conn_id 2001 and flags C         :00:08:38
                              lifetime of 3600 seconds         :00:08:38
                          lifetime of 4608000 kilobytes         :00:08:38
     ISAKMP (0:1): sending packet to 14.38.69.71 (I) QM_IDLE :00:08:38
"" ISAKMP (0:1): deleting node -1119238561 error FALSE reason :00:08:38
  ,ISAKMP (0:1): Node -1119238561, Input = IKE_MESG_FROM_PEER :00:08:38
                                  IKE_QM_EXCH Old State = IKE_QM_I_QM1
                                    New State = IKE_QM_PHASE2_COMPLETE

                        ...IPSEC(key_engine): got a queue event :00:08:38
                                       , :(IPSEC(initialize_sas :00:08:38
    ,key eng. msg.) INBOUND local= 14.38.69.70, remote= 14.38.69.71)
                    ,(local_proxy= 1.1.1.0/255.255.255.0/0/0 (type=4
                   ,(remote_proxy= 2.2.2.0/255.255.255.0/0/0 (type=4
                   , protocol= ESP, transform= esp-3des esp-md5-hmac
                                     ,lifedur= 3600s and 4608000kb
 spi= 0x4B68058A(1265108362), conn_id= 2000, keysize= 0, flags= 0x4
                                       , :(IPSEC(initialize_sas :00:08:38
   ,key eng. msg.) OUTBOUND local= 14.38.69.70, remote= 14.38.69.71)
                    ,(local_proxy= 1.1.1.0/255.255.255.0/0/0 (type=4
                   ,(remote_proxy= 2.2.2.0/255.255.255.0/0/0 (type=4
                   , protocol= ESP, transform= esp-3des esp-md5-hmac
                                     ,lifedur= 3600s and 4608000kb
 spi= 0x59997B2D(1503230765), conn_id= 2001, keysize= 0, flags= 0xC
                                  ,IPSEC(create_sa): sa created :00:08:38
                                ,sa) sa_dest= 14.38.69.70, sa_prot= 50)
                                     ,(sa_spi= 0x4B68058A(1265108362
                 sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2000
                                  ,IPSEC(create_sa): sa created :00:08:38
                                ,sa) sa_dest= 14.38.69.71, sa_prot= 50)
                                     ,(sa_spi= 0x59997B2D(1503230765
                 sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2001
                            (ISAKMP: received ke message (7/1 :00:08:38
                      ISAKMP: DPD received kei with flags 0x10 :00:08:38
                    ISAKMP: Locking DPD struct 0x82702444 from :00:08:38
                            crypto_ikmp_dpd_handle_kei_mess, count 2
```

معلومات ذات صلة

- صفحة دعم IPSec
- الدعم الفني - Cisco Systems

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).