التضمين اليدوي ل IPSec بين مثال تكوين الموجهات

المحتويات

المقدمة

يتيح لك نموذج التكوين هذا تشفير حركة مرور البيانات بين شبكات x.12.12.12 و x.14.14.14 بمساعدة عملية الكبح اليدوي ل IPsec. لأغراض الاختبار، تم إستخدام قائمة التحكم في الوصول (ACL) والاختبار الموسع من المضيف 12.12.12.12 إلى 14.14.14.14.

عادة ما يكون الحفظ اليدوي ضروريا فقط عند تكوين جهاز Cisco لتشفير حركة مرور البيانات إلى جهاز مورد آخر لا يدعم تبادل مفتاح الإنترنت (IKE). إذا كان IKE قابلا للتكوين على كلا الجهازين، فمن المفضل إستخدام ميزة الكبح التلقائي. تكون فهارس معلمات أمان الجهاز (SPIs) من Cisco عشرية ومع ذلك يقوم بعض الموردين بعمل SPIs في وضع الأساس السداسي عشر. إذا كان هذا هو الحال، فأحيانا يلزم التحويل.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات أساسية خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- الموجهات طراز 3640 و 1605 من Cisco
- برنامج IOS® الإصدار a.12.3.3 من Cisco

ملاحظة: في جميع الأنظمة الأساسية التي تحتوي على مهايئات تشفير الأجهزة، لا يكون التشفير اليدوي مدعوما عند تمكين محول تشفير الأجهزة.

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 كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

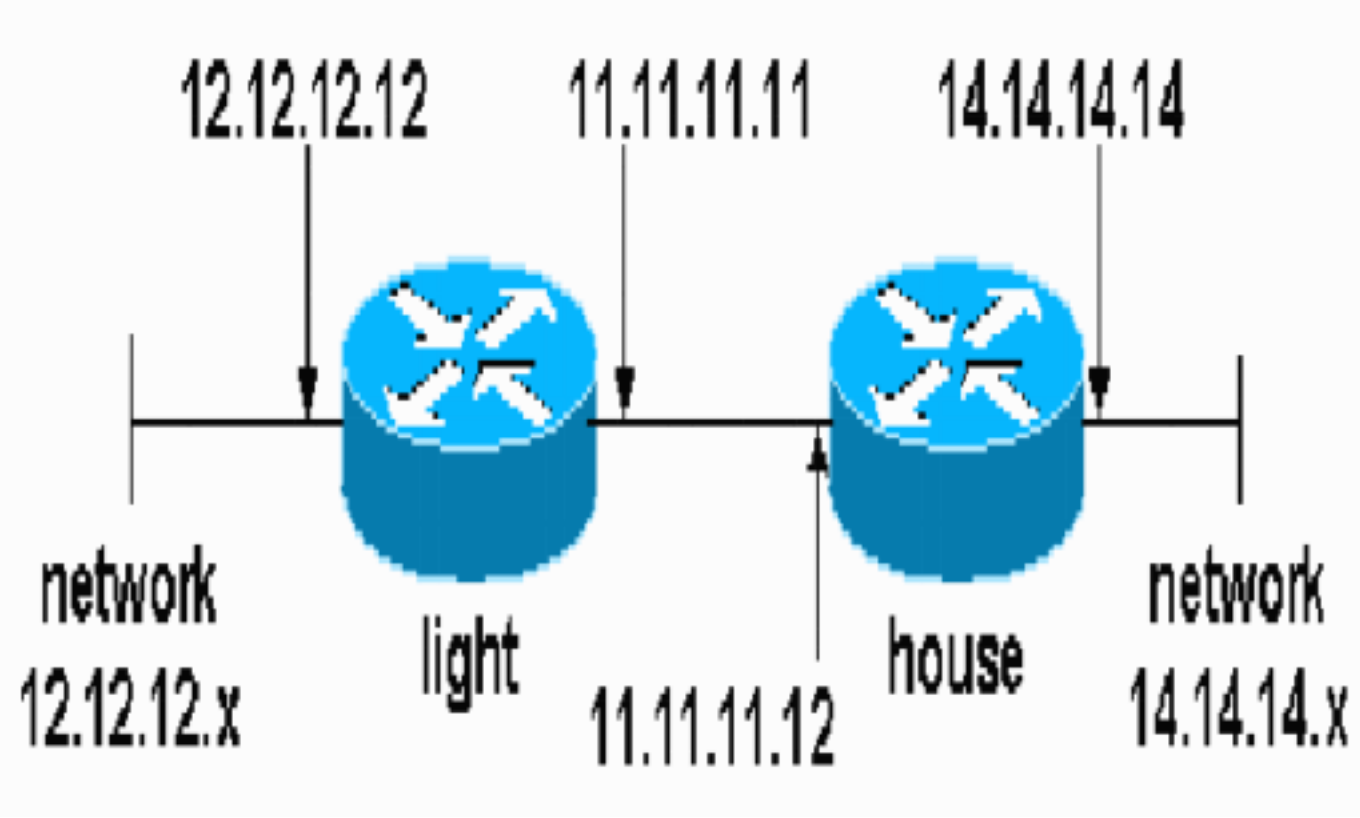
التكوين

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

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للعثور على مزيد من المعلومات حول الأوامر المستخدمة في هذا المستند.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



التكوينات

يستخدم هذا المستند التكوينات التالية:

- تشكيل خفيف
- تهيئة المنزل

تشكيل خفيف

```
light#show running-config
...Building configuration

Current configuration : 1177 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname light
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
no aaa new-model
ip subnet-zero
!
no crypto isakmp enable
IPsec configuration crypto ipsec transform-set ---!!
encrypt-des esp-des esp-sha-hmac
!
!
crypto map testcase 8 ipsec-manual
set peer 11.11.11.12
set session-key inbound esp 1001 cipher
1234abcd1234abcd authenticator 20
set session-key outbound esp 1000 cipher
abcd1234abcd1234 authenticator 20
set transform-set encrypt-des !--- Traffic to encrypt
match address 100
!
!
interface Ethernet2/0
ip address 12.12.12.12 255.255.255.0
!<half-duplex<br
interface Ethernet2/1
ip address 11.11.11.11 255.255.255.0
half-duplex !--- Apply crypto map. crypto map testcase
!
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 11.11.11.12
!
Traffic to encrypt access-list 100 permit ---!          !
ip host 12.12.12.12 host 14.14.14.14
!
!
!
!
line con 0
```

```
line aux 0
line vty 0 4
 login
!
!
!
```

تهيئة المنزل

```
house#show running-config

Current configuration : 1194 bytes
!
version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname house
!
!
logging buffered 50000 debugging
enable password cisco
!
no aaa new-model
ip subnet-zero
ip domain name cisco.com
!
ip cef
!
!
no crypto isakmp enable
!
IPsec configuration crypto ipsec transform-set ---!!
encrypt-des esp-des esp-sha-hmac
!
crypto map testcase 8 ipsec-manual
 set peer 11.11.11.11
 set session-key inbound esp 1000 cipher
 abcd1234abcd1234 authenticator 20
 set session-key outbound esp 1001 cipher
 1234abcd1234abcd authenticator 20
 set transform-set encrypt-des
 Traffic to encrypt match address 100 ---!
!
!
interface Ethernet0
 ip address 11.11.11.12 255.255.255.0!--- Apply crypto
 map. crypto map testcase
!
interface Ethernet1
 ip address 14.14.14.14 255.255.255.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 11.11.11.11
no ip http server
no ip http secure-server
!
Traffic to encrypt access-list 100 permit ip host ---!!
14.14.14.14 host 12.12.12.12
!
!
line con 0
```

```
 exec-timeout 0 0
transport preferred none
 transport output none
 line vty 0 4
 exec-timeout 0 0
 password cisco
 login
transport preferred none
 transport input none
 transport output none
!
!
end
```

التحقق من الصحة

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

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

- **show crypto ipSec**—يعرض المرحلة الثانية من اقترانات الأمان.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

أوامر استكشاف الأخطاء وإصلاحها

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

ملاحظة: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل إستخدام أوامر **debug**.

- **debug crypto ipSec**—يعرض مفاوضات IPsec من المرحلة الثانية.
- **debug crypto engine**—يعرض حركة مرور البيانات التي يتم تشفيرها.

مجموعات التحويل غير متطابقة

الضوء لديه AH-SHA-HMAC و House لديه ESP-DES.

```
                                , :(Mar  2 01:16:09.849: IPSEC(sa_request*
,key eng. msg.) OUTBOUND local= 11.11.11.11, remote= 11.11.11.12)
                ,(local_proxy= 12.12.12.12/255.255.255.255/0/0 (type=1
               ,(remote_proxy= 14.14.14.14/255.255.255.255/0/0 (type=1
                                , protocol= AH, transform= ah-sha-hmac
                                        ,lifedur= 3600s and 4608000kb
spi= 0xACD76816(2899798038), conn_id= 0, keysize= 0, flags= 0x400A
                           :(Mar  2 01:16:09.849: IPSEC(manual_key_stuffing*
                      .....keys missing for addr 11.11.11.12/prot 51/spi 0
```

قوائم التحكم في الوصول (ACL) غير متطابقة

على side_a (الموجه "الضوء") هناك مضيف إلى الداخل-مضيف وعلى الجانب_b (موجه "المنزل") هناك واجهة إلى واجهة. يجب أن تكون قوائم التحكم في الوصول (ACL) متماثلة دائما (هذه ليست).

```
hostname house
match address 101
access-list 101 permit ip host 11.11.11.12 host 11.11.11.11
!

hostname light
match address 100
access-list 100 permit ip host 12.12.12.12 host 14.14.14.14
```

هذا المخرج مأخوذ من SIDE_A بدء إختبار الاتصال:

```
nothing

light#show crypto engine connections active

ID Interface       IP-Address      State  Algorithm           Encrypt  Decrypt
Ethernet2/1     11.11.11.11     set    DES_56_CBC             5        0 2000
Ethernet2/1     11.11.11.11     set    DES_56_CBC             0        0 2001
```

يتم أخذ هذا الإخراج من الجانب_b عندما يقوم الجانب_A بتهيئة ping:

```
#house
1d00h: IPSEC(epa_des_crypt): decrypted packet failed SA identity check
1d00h: IPSEC(epa_des_crypt): decrypted packet failed SA identity check
1d00h: IPSEC(epa_des_crypt): decrypted packet failed SA identity check
1d00h: IPSEC(epa_des_crypt): decrypted packet failed SA identity check
1d00h: IPSEC(epa_des_crypt): decrypted packet failed SA identity check

house#show crypto engine connections active

  ID Interface       IP-Address      State  Algorithm           Encrypt  Decrypt
Ethernet0       11.11.11.12     set    DES_56_CBC             0        0 2000
 Ethernet0       11.11.11.12     set    DES_56_CBC             0        5 2001
```

هذا المخرج مأخوذ من الجانب_b الذي يقوم بتشغيل ping:

```
side_ B

.CRYPTO-4-RECVD_PKT_NOT_IPSEC: Rec'd packet not an IPSEC packet%
ip) vrf/dest_addr= /12.12.12.12, src_addr= 14.14.14.14, prot= 1)
```

أحد الطرفين يحتوي على خريطة تشفير والآخر لا يحتوي على

```
.CRYPTO-4-RECVD_PKT_NOT_IPSEC: Rec'd packet not an IPSEC packet%
ip) vrf/dest_addr= /14.14.14.14, src_addr= 12.12.12.12, prot= 1)
```

هذا المخرج مأخوذ من side_b الذي يحتوي على خريطة تشفير:

```
house#show crypto engine connections active
 ID Interface       IP-Address      State  Algorithm           Encrypt  Decrypt
Ethernet0       11.11.11.12     set    DES_56_CBC             5        0 2000
Ethernet0       11.11.11.12     set    DES_56_CBC             0        0 2001
```

تم تمكين بطاقة مسرع محرك التشفير

```
1d05h: %HW_VPN-1-HPRXERR: Hardware VPN0/13: Packet
    .....Encryption/Decryption error, status=4098
```

معلومات ذات صلة

- مفاوضة IPSec/بروتوكولات IKE
- الدعم التقني والمستندات - 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).