تكوين بروتوكول IPSec من موجه إلى موجه ديناميكي إلى ساكن إستاتيكي باستخدام NAT

المحتويات

المقدمة

في نموذج التكوين هذا، يستقبل الموجه البعيد عنوان IP من خلال جزء من PPP يسمى بروتوكول التحكم في بروتوكول الإنترنت (IPCP). يستخدم الموجه البعيد عنوان IP للاتصال بموجه صرة. يتيح هذا التكوين لموجه الموزع قبول إتصالات IPSec الديناميكية. يستخدم الموجه عن بعد ترجمة عنوان الشبكة (NAT) "للانضمام" إلى الأجهزة التي تتم مخاطبتها بشكل خاص ووراءه إلى الشبكة ذات العناوين الخاصة خلف الموجه الرئيسي. يعرف الموجه عن بعد نقطة النهاية ويمكن أن يبدأ الاتصالات بموجه الموزع. ولكن موجه الموزع لا يعرف نقطة النهاية، لذلك لا يمكنه بدء الاتصالات بالموجه البعيد.

في هذا المثال، يمثل dr_whoovie الموجه البعيد ويمثل sam-i-am موجه الموزع. تحدد قائمة حركة المرور التي سيتم تشفيرها، لذلك يعرف dr_whoovie الوصول إلى sam-i-am. يجب أن يقوم الموجه البعيد بدء الاتصال. كلا الطرفين يقومون بحمل زائد ل NAT.

المتطلبات الأساسية

المتطلبات

يتطلب هذا المستند فهما أساسيا لبروتوكول IPSec. لمعرفة المزيد حول IPSec، يرجى الرجوع إلى مقدمة لتشفير أمان IP (IPSec).

المكونات المستخدمة

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

- برنامج IOS® الإصدار 12.2(24a) من Cisco
- الموجّهات من السلسلة 2500 من Cisco

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 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: استخدم 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:

- أم-آي-ماس
- يفوه د


```
!--- Use dynamic crypto maps to create policy templates !--- that can be used to process negotiation re
```

يفوه_د

```
command !--- in global configuration mode. !--- IKE po

!--

!--- A transform set is an acceptable combination !--- of security protocols and algorithms. !---
```

```
                    !--- Creates a crypto map and indicates that IKE will be used !--- to establ

                                                                                                !---

                                                                                                !--- I

                                                                                    !--- This indicates that the int

!--- Specifies that the IP address for this interface !--- is obtained via PPP/IPCP address negotiatio
```

```
interface cont

!--- I
```

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.

- ping —يستخدم لتشخيص الاتصال الأساسي بالشبكة

يوضح هذا المثال إختبار اتصال من واجهة إيثرنت 10.1.1.1 على dr_whoovie إلى واجهة إيثرنت 10.2.2.3 على sam-i-am.

```
<#root>

dr_whoovie#

ping

                                        Protocol [ip]:
                                Target IP address: 10.2.2.3
                                   Repeat count [5]:
                                 Datagram size [100]:
                                Timeout in seconds [2]:
                              Extended commands [n]: y
                        Source address or interface: 10.1.1.1
                                    Type of service [0]:
                               Set DF bit in IP header? [no]:
                                  Validate reply data? [no]:
                                      Data pattern [0xABCD]:
                    Loose, Strict, Record, Timestamp, Verbose[none]:
                                  Sweep range of sizes [n]:
                                Type escape sequence to abort.
                            Sending 5, 100-byte ICMP Echos to 10.2.2.3,
                                           timeout is 2 seconds:
                       Packet sent with a source address of 10.1.1.1
                                                           !!!!!
                                  Success rate is 100 percent (5/5),
                                round-trip min/avg/max = 36/38/40 ms
```

- show crypto ipSec — يعرض اقترانات أمان المرحلة 2 (SA).
- show crypto isakmp sa — يعرض المرحلة 1 SAs.

نموذج الإخراج

هذا المخرج من الأمر show crypto ipSec sa الصادر على موجه الموزع.

```
<#root>

sam-i-am#

show crypto ipsec sa


                                        interface: Serial0
                            Crypto map tag: rtptrans, local addr. 99.99.99.1


      local  ident (addr/mask/prot/port): (10.2.2.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)

                                        current_peer: 100.100.100.1
                                              PERMIT, flags={}
                          #pkts encaps: 6, #pkts encrypt: 6, #pkts digest 6
                          #pkts decaps: 6, #pkts decrypt: 6, #pkts verify 6
                                 #pkts compressed: 0, #pkts decompressed: 0
                           #pkts not compressed: 0, #pkts compr. failed: 0,
                #pkts decompress failed: 0, #send errors 0, #recv errors 0
```

```
local crypto endpt.: 99.99.99.1, remote crypto endpt.: 100.100.100.1
path mtu 1500, ip mtu 1500, ip mtu interface Serial0
current outbound spi: 52456533

inbound esp sas:
spi: 0x6462305C(1684156508)
transform: esp-des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2000, flow_id: 1, crypto map: rtptrans
sa timing: remaining key lifetime (k/sec): (4607999/3510)
IV size: 8 bytes
replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x52456533(1380279603)
transform: esp-des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2001, flow_id: 2, crypto map: rtptrans
sa timing: remaining key lifetime (k/sec): (4607999/3510)
IV size: 8 bytes
replay detection support: Y

outbound ah sas:

outbound pcp sas:
```

قفنلا لصتي .ةريظنلا ةزهجألا نيب اهؤاشنإ مت يتلا IPSec SAs لئاسر رمألا اذه ضرعي اذه لمحي .sam-i-am ىلع 99.99.99.1 ةهجاوو dr_whoovie ىلع 100.100.100.1 ةهجاوب رفشملا نامأ ليمحت يطيسو ءاشنإ مت .10.1.1.1 و 10.2.2.3 تاكبشلا نيب تانايبلا رورم ةكرح قفنلا فرعي ال sam-i-am نأ نم مغرلا ىلع قفنلا ءاشنإ متي .رداصلاو لخادلل (ESP) نيمضتلا (AH) ةقداصملا سأرب ةصاخلا SA تاكبش مادختسإ متي ال .(100.100.100.1) ريظنلل IP ناونع AH. نيوكت مدعل ارظن

IP ناونع ىقلتت dr_whoovie ىلع 0 ةيلسلستلا ةهجاولا نأ هذه تاجرخملا جذامن حضوت IPCP. لالخ نم 100.100.100.1 ةميقب

- :IP ناونع ىلع ضوافتلا لبق

<#root>

```
dr_whoovie#
```

```
show interface serial0

Serial0 is up, line protocol is up
Hardware is HD64570

Internet address will be negotiated using IPCP

MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, loopback not set
```

- بعد التفاوض على عنوان IP:

```
<#root>

dr_whoovie#

show interface serial0

Serial0 is up, line protocol is up
Hardware is HD64570

Internet address is 100.100.100.1/32

MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, loopback not set
```

تم إعداد هذا المثال في مختبر باستخدام الأمر peer default ip address لتخصيص عنوان IP في الطرف البعيد من الواجهة 0 التسلسلية على dr_whoovie. يتم تحديد تجمع IP باستخدام الأمر ip local pool في الطرف البعيد.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

أوامر استكشاف الأخطاء وإصلاحها

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

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

- debug crypto ipSec — يعرض مفاوضات IPSec للمرحلة 2.
- debug crypto isakmp — يعرض مفاوضات بروتوكول إدارة المفاتيح وارتباط الأمان للمرحلة الأولى (ISAKMP) عبر الإنترنت.
- debug crypto Engine — يعرض حركة مرور البيانات التي يتم تشفيرها.

- debug ip nat detail — (إختياري) يتحقق من تشغيل ميزة NAT عن طريق عرض معلومات حول كل حزمة يقوم الموجه بترجمتها.

  تحذير: يقوم هذا الأمر بإنشاء كمية كبيرة من الإخراج. أستخدم هذا الأمر فقط عندما تكون حركة المرور على شبكة IP منخفضة.

- مسح التشفير isakmp — يعمل على مسح مناطق الوصول (SAs) المتعلقة بالمرحلة الأولى.

- مسح التشفير sa — يمحو الاختالالت المتعلقة بالمرحلة 2.

- واضح ip nat ترجمة — يمحو ترجمة nat ديناميكية من الترجمة طاولة.

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).