تكوين موجه إلى موجه IPSec، مشترك مسبقا، وعامة خاصة بين شبكة NAT لـ زائد حمل

المحتويات

المقدمة

يوضح هذا التكوين النموذجي كيفية تشفير حركة مرور البيانات بين شبكة خاصة (x.10.103.1) وشبكة عامة (x.98.98.98) باستخدام IPSec. تعرف شبكة x.98.98.98 شبكة x.10.103.1 عن طريق العناوين الخاصة. تعرف شبكة x.10.103.1 شبكة x.98.98.98 عن طريق العناوين العامة.

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 Cisco IOS® الإصدار 12.3(5) من Cisco
- موجهات Cisco 3640

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.

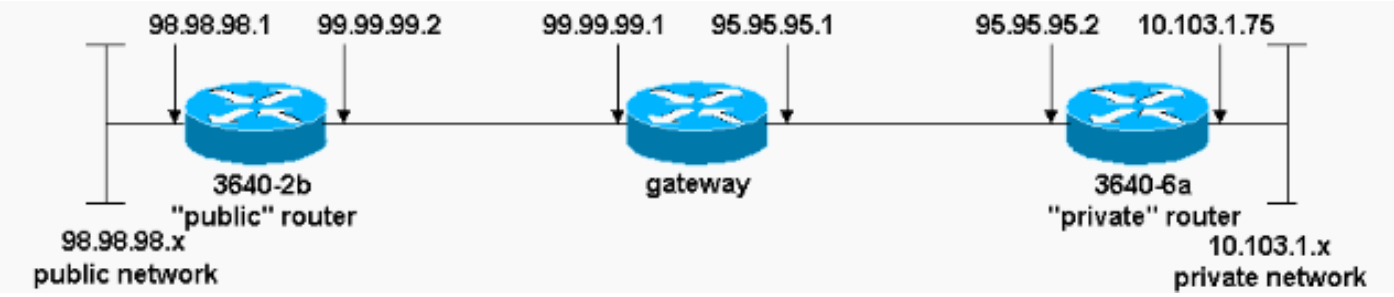
التكوين

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 هذا الرسم التخطيطي.



التكوينات

يستخدم هذا المستند التكوينات التالية:

- الموجه 2B-3640 "العام"
- الموجه 6A-3640 "الخاص"

الموجه 2B-3640 "العام"

```
rp-3640-2b#show running config
...Building configuration

:Current configuration
!
version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname rp-3640-2b
!
ip subnet-zero
!


!
Defines the Internet Key Exchange (IKE) policies. ---!
crypto isakmp policy 1

Defines an IKE policy. Use the crypto isakmp policy ---!
!--- command in global configuration mode. IKE policies
```

```
!--- define a set of parameters !--- that are used
.during the IKE phase I negotiation


                                                hash md5
                                  authentication pre-share

    Specifies preshared keys as the authentication ---!
  method. crypto isakmp key cisco123 address 95.95.95.2

 Configures a preshared authentication key, used in ---!
         !--- global configuration mode. ! crypto ipsec
                  transform-set rtpset esp-des esp-md5-hmac

Defines a transform-set. This is an acceptable !--- ---!
  combination of security protocols and algorithms, !---
which has to be matched on the peer router. ! crypto map
                                        rtp 1 ipsec-isakmp

   Indicates that IKE is used to !--- establish the ---!
 IPSec security associations (SAs) that protect !--- the
    traffic specified by this crypto map entry. set peer
                                                95.95.95.2

        Sets the IP address of the remote end. set ---!
                                      transform-set rtpset

     Configures IPSec to use the transform-set !--- ---!
            "rtpset" defined earlier. match address 115

This is used to assign an extended access list to a ---!
    !--- crypto map entry which is used by IPSec !--- to
     determine which traffic should be protected !--- by
      crypto and which traffic does not !--- need crypto
          protection. ! interface Ethernet0/0 ip address
     98.98.98.1 255.255.255.0 no ip directed-broadcast !
                                    interface Ethernet0/1
                  ip address 99.99.99.2 255.255.255.0
                                 no ip directed-broadcast
                                       no ip route-cache

 Enable process switching for !--- IPSec to encrypt ---!
       outgoing packets. !--- This command disables fast
            switching. no ip mroute-cache crypto map rtp

Configures the interface to use !--- the crypto map ---!
   "rtp" for IPSec. ! . . !--- Output suppressed. . . ip
          classless ip route 0.0.0.0 0.0.0.0 99.99.99.1

  Default route to the next hop address. no ip http ---!
 server ! access-list 115 permit ip 98.98.98.0 0.0.0.255
                                          10.103.1.0 0.0.0.255

 This access-list option causes all IP traffic !--- ---!
        that matches the specified conditions to be !---
   protected by IPSec using the policy described by !---
       .the corresponding crypto map command statements


        access-list 115 deny ip 98.98.98.0 0.0.0.255 any

                                                         !
                                                 line con 0
                                          transport input none
```

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

الموجه 6A-3640 "الخاص"

```
rp-3640-6a#show running config
...Building configuration

:Current configuration
!
version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname rp-3640-6a
!

!
ip subnet-zero



Defines the IKE policies. ! crypto isakmp policy 1 ---!

Defines an IKE policy. !--- Use the crypto isakmp ---!
policy !--- command in global configuration mode. IKE
policies !--- define a set of parameters !--- that are
.used during the IKE phase I negotiation


hash md5
authentication pre-share

Specifies preshared keys as the authentication ---!
method. crypto isakmp key cisco123 address 99.99.99.2

Configures a preshared authentication key, !--- ---!
used in global configuration mode. ! crypto ipsec
transform-set rtpset esp-des esp-md5-hmac

Defines a transform-set. This is an !--- acceptable ---!
combination of security protocols and algorithms, !---
which has to be matched on the peer router. crypto map
rtp 1 ipsec-isakmp

Indicates that IKE is used to establish !--- the ---!
IPSec SAs that protect the traffic !--- specified by
this crypto map entry. set peer 99.99.99.2

Sets the IP address of the remote end. set ---!
transform-set rtpset

Configures IPSec to use the transform-set !--- ---!
"rtpset" defined earlier. match address 115

Used to assign an extended access list to a !--- ---!
crypto map entry which is used by IPSec !--- to
determine which traffic should be protected !--- by
crypto and which traffic does not !--- need crypto
```

```
protection. . . !--- Output suppressed. . . ! interface
  Ethernet3/0 ip address 95.95.95.2 255.255.255.0 no ip
                        directed-broadcast ip nat outside

 Indicates that the interface is !--- connected to ---!
                  the outside network. no ip route-cache

 Enable process switching for !--- IPSec to encrypt ---!
       outgoing packets. !--- This command disables fast
            switching. no ip mroute-cache crypto map rtp

Configures the interface to use the !--- crypto map ---!
     "rtp" for IPSec. ! interface Ethernet3/2 ip address
  10.103.1.75 255.255.255.0 no ip directed-broadcast ip
                                              nat inside

  Indicates that the interface is connected to !--- ---!
          the inside network (the network subject to NAT
translation). ! ip nat pool FE30 95.95.95.10 95.95.95.10
                                      netmask 255.255.255.0

Used to define a pool of IP addresses for !--- NAT. ---!
Use the ip nat pool command in !--- global configuration
                                                  .mode


 ip nat inside source route-map nonat pool FE30 overload

      Used to enable NAT of !--- the inside source ---!
  address. Use the ip nat inside source !--- command in
  global configuration mode. !--- The 'overload' option
  enables the router to use one global !--- address for
                                       .many local addresses


                                              ip classless
                        ip route 0.0.0.0 0.0.0.0 95.95.95.1

 Default route to the next hop address. no ip http ---!
  server ! access-list 110 deny ip 10.103.1.0 0.0.0.255
                                      98.98.98.0 0.0.0.255
      access-list 110 permit ip 10.103.1.0 0.0.0.255 any

 Addresses that match this ACL are NATed while !--- ---!
    they access the Internet. They are not NATed !--- if
     they access the 98.98.98.0 network. access-list 115
     permit ip 10.103.1.0 0.0.0.255 98.98.98.0 0.0.0.255

 This access-list option causes all IP traffic that ---!
       !--- matches the specified conditions to be !---
   protected by IPSec using the policy described !--- by
       .the corresponding crypto map command statements


       access-list 115 deny ip 10.103.1.0 0.0.0.255 any

                                  route-map nonat permit 10
                                       match ip address 110
                                                          !

                                                          !
                                                  line con 0
```

```
line vty 0 4

!
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**.

للتحقق من هذا التكوين، جرب الأمر **ping** الموسع المستمد من واجهة إيثرنت على الموجه الخاص 10.103.1.75، الموجه إلى واجهة الإيثرنت على الموجه العام 98.98.98.1

- ping —يستخدم لتشخيص الاتصال الأساسي بالشبكة.

```
rp-3640-6a#ping
:[Protocol [ip
Target IP address: 98.98.98.1
:[Repeat count [5
:[Datagram size [100
:[Timeout in seconds [2
Extended commands [n]: y
Source address or interface: 10.103.1.75
:[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 98.98.98.1, timeout is 2 seconds
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 64/64/68 ms
```

- show crypto ipSec — يعرض الإعدادات المستخدمة من قبل IPSec) SAs) الحالية.
- show crypto isakmp sa — يعرض جميع شبكات IKE الحالية في نظير.
- show crypto engine — يعرض ملخصا لمعلومات التكوين لمحركات التشفير. أستخدم الأمر **show crypto engine** في وضع EXEC ذي الامتيازات.

نموذج عرض الإخراج

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

```
rp-3640-6a#show crypto ipsec sa

interface: Ethernet0/0
Crypto map tag: rtp, local addr. 95.95.95.2

:protected vrf
(local  ident (addr/mask/prot/port): (10.103.1.0/255.255.255.0/0/0
(remote ident (addr/mask/prot/port): (98.98.98.0/255.255.255.0/0/0
current_peer: 99.99.99.2:500
{,PERMIT, flags={origin_is_acl
pkts encaps: 5, #pkts encrypt: 5, #pkts digest 5#
pkts decaps: 14, #pkts decrypt: 14, #pkts verify 14#
pkts compressed: 0, #pkts decompressed: 0#
```

```
                                pkts not compressed: 0, #pkts compr. failed: 0#
                              pkts not decompressed: 0, #pkts decompress failed: 0#
                                                    send errors 0, #recv errors 0#

local crypto endpt.: 95.95.95.2, remote crypto endpt.: 99.99.99.2
                                                  path mtu 1500, media mtu 1500
                                                current outbound spi: 75B6D4D7

                                                                 :inbound esp sas
                                                   (spi: 0x71E709E8(1910966760
                                               , transform: esp-des esp-md5-hmac
                                                    { ,in use settings ={Tunnel
                                     slot: 0, conn id: 2000, flow_id: 1, crypto map: rtp
                                (sa timing: remaining key lifetime (k/sec): (4576308/3300
                                                                IV size: 8 bytes
                                                  replay detection support: Y

                                                                :inbound ah sas

                                                                :inbound pcp sas

                                                                :outbound esp sas
                                                   (spi: 0x75B6D4D7(1974916311
                                               , transform: esp-des esp-md5-hmac
                                                    { ,in use settings ={Tunnel
                                     slot: 0, conn id: 2001, flow_id: 2, crypto map: rtp
                                (sa timing: remaining key lifetime (k/sec): (4576310/3300
                                                                IV size: 8 bytes
                                                  replay detection support: Y

                                                                :outbound ah sas

                                                                :outbound pcp sas
```

يعرض هذا الأمر رسائل IPSec SAs التي تم إنشاؤها بين الأقران. يتم إنشاء النفق المشفر بين 95.95.95.2 و 99.99.99.2 لحركة المرور التي تنتقل بين الشبكات 98.98.98.0 و 10.103.1.0. يمكنك رؤية وحمولة أمان التضمين (ESP) SAs التي تم إنشاؤها داخليا وخارجيا. لا يتم إستخدام أسماء SA الخاصة برأس المصادقة (AH) نظرا لعدم وجود أي AHs.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

أوامر استكشاف الأخطاء وإصلاحها

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

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

- **debug crypto ipSec sa**— **يستخدم** للاطلاع على مفاوضات IPSec الخاصة بالمرحلة 2.
- **debug crypto isakmp sa**— **يستخدم** للاطلاع على مفاوضات ISAKMP الخاصة بالمرحلة 1.
- **debug crypto engine**—يستخدم لعرض الجلسات المشفرة.

معلومات ذات صلة

- ترتيب عملية NAT
- أستكشاف أخطاء أمان IP وإصلاحها - فهم أوامر التصحيح واستخدامها
- صفحة دعم IPSec
- صفحة دعم ترجمة عناوين الشبكة (NAT)
- 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).