تكوين موجه إلى موجه IPSec مع التحميل الزائد ل NAT وعميل VPN الآمن من Cisco

المحتويات

المقدمة

يقوم هذا التكوين العينة بتشفير حركة مرور البيانات من الشبكة خلف الضوء إلى الشبكة خلف المنزل (الشبكة 192.168.100.x إلى 192.168.200.x). يتم أيضا تنفيذ الحمل الزائد لترجمة عنوان الشبكة (NAT). يتم السماح باتصالات عميل VPN المشفرة في Light مع بطاقة برية ومفاتيح مشتركة مسبقا و mode-config. تتم ترجمة حركة المرور إلى الإنترنت، ولكن ليس مشفرة.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- برنامج IOS® الإصدار 12.2.7 و 12.2.8T من Cisco
- Cisco Secure VPN Client 1.1 (يظهر على أنه 2.1.12 في قائمة **تعليمات** عميل **About < IRE**)
- الموجهات 3600 من Cisco**ملاحظة:** إذا كنت تستخدم الموجهات من السلسلة Cisco 2600 Series لهذا النوع من سيناريو VPN، فيجب تثبيت الموجهات باستخدام صور IOS الخاصة ب IPsec VPN المشفرة.

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.

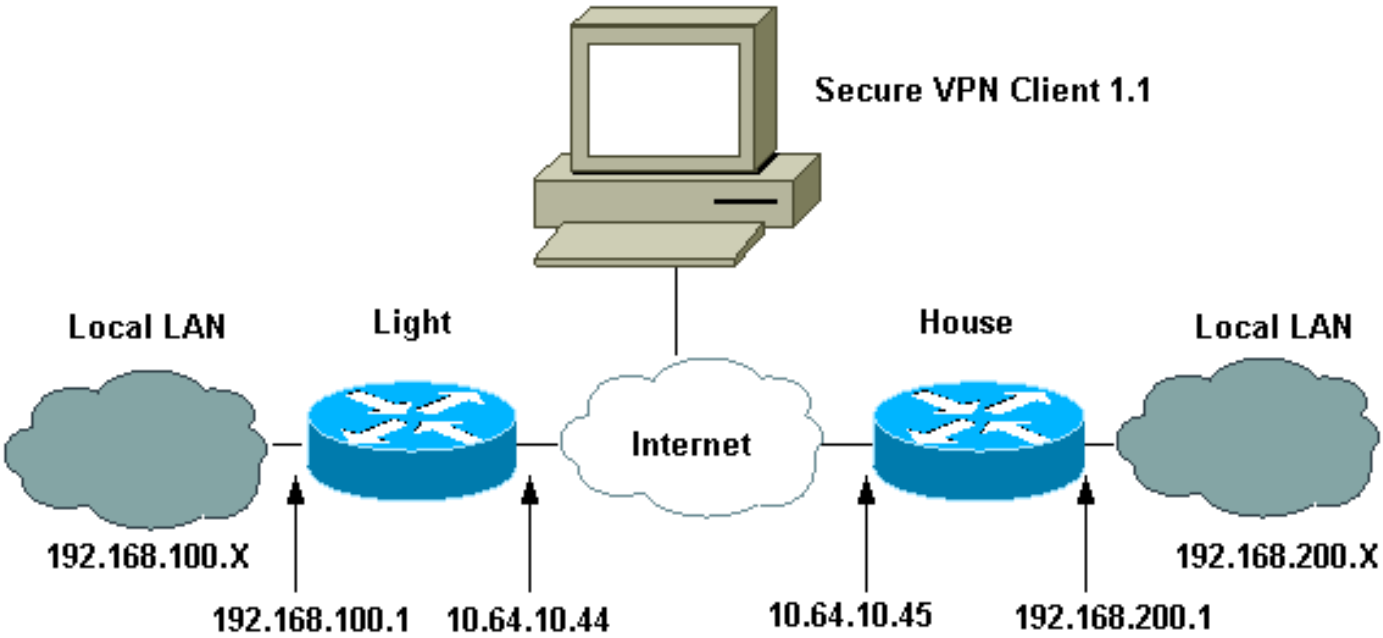
التكوين

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

ملاحظة: 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 هذه التكوينات.

- تشكيل خفيف
- تهيئة المنزل
- تكوين عميل شبكة VPN

تشكيل خفيف

```
Current configuration : 2047 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Light
```

```
!
boot system flash:c3660-ik9o3s-mz.122-8T
!
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
ip ssh time-out 120
ip ssh authentication-retries 3
!
IPsec Internet Security Association and !--- Key ---!
   Management Protocol (ISAKMP) policy. crypto isakmp
policy 5
hash md5
authentication pre-share
   ISAKMP key for static LAN-to-LAN tunnel !--- ---!
without extended authenticaton (xauth). crypto isakmp
key cisco123 address 10.64.10.45 no-xauth
   ISAKMP key for the dynamic VPN Client. crypto ---!
isakmp key 123cisco address 0.0.0.0 0.0.0.0
   Assign the IP address to the VPN Client. crypto ---!
isakmp client configuration address-pool local test-pool
!
!
!
crypto ipsec transform-set testset esp-des esp-md5-hmac
!
crypto dynamic-map test-dynamic 10
set transform-set testset
!
!
   VPN Client mode configuration negotiation, !--- ---!
such as IP address assignment and xauth. crypto map test
client configuration address initiate
crypto map test client configuration address respond
Static crypto map for the LAN-to-LAN tunnel. crypto ---!
map test 5 ipsec-isakmp
set peer 10.64.10.45
set transform-set testset
   Include the private network-to-private network ---!
traffic !--- in the encryption process. match address
115
Dynamic crypto map for the VPN Client. crypto map ---!
test 10 ipsec-isakmp dynamic test-dynamic
!


call rsvp-sync
!
!
!
!
!
fax interface-type modem
mta receive maximum-recipients 0
!
controller E1 2/0
!
!
!
interface FastEthernet0/0
ip address 10.64.10.44 255.255.255.224
ip nat outside
duplex auto
```

```
speed auto
crypto map test
!
interface FastEthernet0/1
ip address 192.168.100.1 255.255.255.0
ip nat inside
duplex auto
speed auto
!
interface BRI4/0
no ip address
shutdown
!
interface BRI4/1
no ip address
shutdown
!
interface BRI4/2
no ip address
shutdown
!
interface BRI4/3
no ip address
shutdown
!
Define the IP address pool for the VPN Client. ip ---!
local pool test-pool 192.168.1.1 192.168.1.254
Exclude the private network and VPN Client !--- ---!
traffic from the NAT process. ip nat inside source
route-map nonat interface FastEthernet0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 10.64.10.33
ip http server
ip pim bidir-enable
!
Exclude the private network and VPN Client !--- ---!
traffic from the NAT process. access-list 110 deny   ip
192.168.100.0 0.0.0.255 192.168.200.0 0.0.0.255
access-list 110 deny   ip 192.168.100.0 0.0.0.255
192.168.1.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255 any
Include the private network-to-private network ---!
traffic !--- in the encryption process. access-list 115
permit ip 192.168.100.0 0.0.0.255 192.168.200.0
0.0.0.255
!
Exclude the private network and VPN Client !--- ---!
traffic from the NAT process. route-map nonat permit 10
match ip address 110
!
!
dial-peer cor custom
!
!
!
!
!
line con 0
line 97 108
line aux 0
line vty 0 4
!
end
```

تهيئة المنزل

```
Current configuration : 1689 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname house
!
boot system flash:c3660-jk8o3s-mz.122-7.bin
!
ip subnet-zero
!
!
no ip domain-lookup
!
ip audit notify log
ip audit po max-events 100
ip ssh time-out 120
ip ssh authentication-retries 3
!
IPsec ISAKMP policy. crypto isakmp policy 5 ---!
hash md5
authentication pre-share
ISAKMP key for static LAN-to-LAN tunnel without ---!
xauth authenticaton. crypto isakmp key cisco123 address
10.64.10.44 no-xauth
!
!
crypto ipsec transform-set testset esp-des esp-md5-hmac
!
Static crypto map for the LAN-to-LAN tunnel. crypto ---!
map test 5 ipsec-isakmp
set peer 10.64.10.44
set transform-set testset
Include the private network-to-private network ---!
traffic !--- in the encryption process.  match address
115
!
call rsvp-sync
cns event-service server
!
!
!
!
!
fax interface-type modem
mta receive maximum-recipients 0
!
!
!
interface FastEthernet0/0
ip address 10.64.10.45 255.255.255.224
ip nat outside
duplex auto
speed auto
crypto map test
!
interface FastEthernet0/1
ip address 192.168.200.1 255.255.255.0
ip nat inside
```

```
duplex auto
speed auto
!
interface BRI2/0
no ip address
shutdown
!
interface BRI2/1
no ip address
shutdown
!
interface BRI2/2
no ip address
shutdown
!
interface BRI2/3
no ip address
shutdown
!
interface FastEthernet4/0
no ip address
shutdown
duplex auto
speed auto
!
!--- Exclude the private network traffic from the
!--- dynamic (dynamic association to a pool) NAT process.
ip nat inside source route-map nonat interface FastEthernet0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 10.64.10.33
no ip http server
ip pim bidir-enable
!
!--- Exclude the private network traffic from the NAT process.
access-list 110 deny   ip 192.168.200.0 0.0.0.255 192.168.100.0 0.0.0.255
access-list 110 permit ip 192.168.200.0 0.0.0.255 any
!--- Include the private network-to-private network
!--- traffic in the encryption process.
access-list 115 permit ip 192.168.200.0 0.0.0.255 192.168.100.0 0.0.0.255
!--- Exclude the private network traffic from the NAT process.
route-map nonat permit 10
match ip address 110
!
!
!
dial-peer cor custom
!
!
!
!
!
line con 0
line aux 0
line vty 0 4
login
!
end
```

تكوين عميل شبكة VPN

```
                                    :Network Security policy
                                           TOLIGHT 1-
                                         My Identity
                                Connection security: Secure
                            Remote Party Identity and addressing
                                        ID Type: IP subnet
                                             192.168.100.0
                                             255.255.255.0
                                      Port all Protocol all

                                   Connect using secure tunnel
                                    ID Type: IP address
                                            10.64.10.44


                                       Pre-shared Key=123cisco


                                  (Authentication (Phase 1
                                           Proposal 1
                        Authentication method: pre-shared key
                                        Encryp Alg: DES
                                          Hash Alg: MD5
                                SA life: Unspecified
                                          Key Group: DH 1


                                    (Key exchange (Phase 2
                                         Proposal 1
                                    Encapsulation ESP
                                     Encrypt Alg: DES
                                        Hash Alg: MD5
                                        Encap: tunnel
                                SA life: Unspecified
                                               no AH


                                    Other Connections 2-
                            Connection security: Non-secure
                                Local Network Interface
                                           Name: Any
                                        IP Addr: Any
                                           Port: All
```

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل 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 2 اقترانات الأمان (SAs).
- **show crypto isakmp sa**—يعرض المرحلة 1 SAs.

استكشاف الأخطاء وإصلاحها

أستخدم هذا القسم 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 للمرحلة 2.
- **debug crypto isakmp**—يعرض مفاوضات ISAKMP للمرحلة 1.
- **debug crypto engine**—يعرض حركة مرور البيانات التي يتم تشفيرها.
- **مسح التشفير isakmp**—يعمل على مسح SAs المتعلقة بالمرحلة 1.
- **مسح التشفير sa**—يمسح أسماء مناطق الوصول (SA) المتعلقة بالمرحلة 2.

معلومات ذات صلة

- تكوين أمان شبكة IPSec
- تكوين بروتوكول أمان Internet Key Exchange
- مفاوضة IPsec/صفحة دعم بروتوكول IKE
- صفحات دعم عميل شبكة VPN الآمنة من Cisco
- 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).