تكوين Cisco 827 ل PPPoE مع التحميل الزائد ل VPN IPSec NAT

المحتويات

المقدمة
قبل البدء
الاصطلاحات
المتطلبات الأساسية
المكونات المستخدمة
التكوين
الرسم التخطيطي للشبكة
التكوينات
التحقق من الصحة
استكشاف الأخطاء وإصلاحها
أوامر استكشاف الأخطاء وإصلاحها
معلومات ذات صلة

المقدمة

عادة ما يكون الموجه Cisco 827 جهاز أماكن عمل عميل (CPE) DSL). في نموذج التكوين هذا، يتم تكوين المحول Cisco 827 لبروتوكول الاتصال من نقطة إلى نقطة عبر الإيثرنت (PPPoE) ويتم إستخدامه كنظير في نفق IPSec من شبكة LAN إلى شبكة LAN باستخدام موجه Cisco 3600. ال cisco 827 أيضا يعمل شبكة عنوان ترجمة (nat) حمل زائد أن يزود توصيل الإنترنت لشبكته الداخلية.

قبل البدء

الاصطلاحات

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

المتطلبات الأساسية

عند النظر في هذا التكوين، يرجى تذكر ما يلي.

- تأكد من عمل PPPoE قبل إضافة تكوين ل IPSec VPN في Cisco 827. لتصحيح أخطاء عميل PPPoE على Cisco 827، يجب مراعاة مكدس البروتوكولات. يجب أستكشاف الأخطاء وإصلاحها في التسلسل أدناه.الطبقة المادية ل DSLطبقة ATMطبقة إيثرنتطبقة PPP
- في هذا عينة تشكيل، ال cisco 827 يتلقى عنوان ساكن إستاتيكي. إذا كان Cisco 827 لديك عنوان IP ديناميكي، فالرجاء مراجعة تكوين IPSec من موجه إلى موجه ديناميكي إلى ساكن إستاتيكي باستخدام NAT بالإضافة إلى هذا المستند.

المكونات المستخدمة

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

- Cisco 827، الإصدار YB4(5)12.1
- Cisco 3600، الإصدار T8(5)12.1
- Cisco 6400، الإصدار DC1(1)12.1

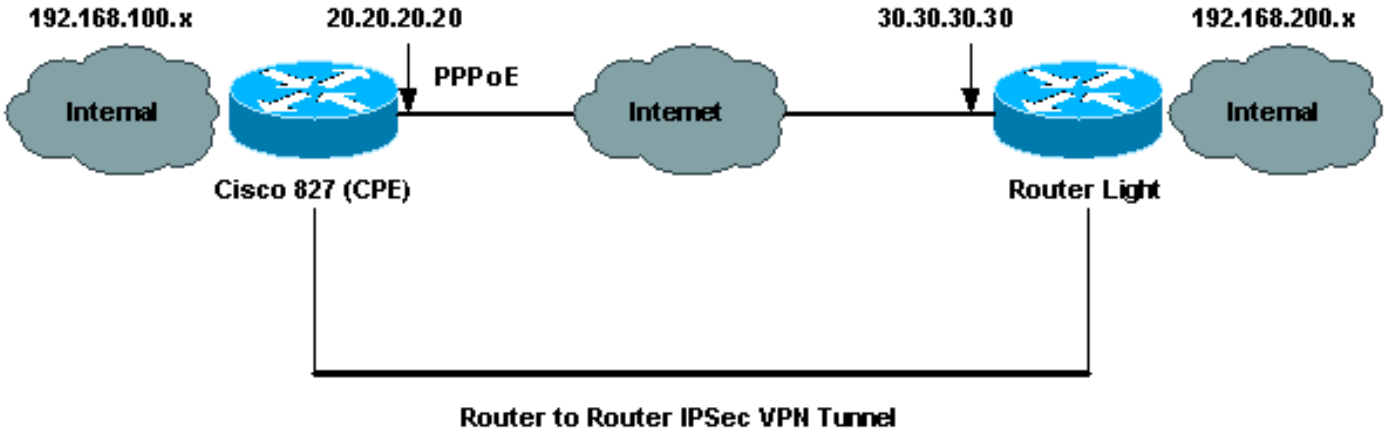
تم إنشاء المعلومات المُقدمة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كنت تعمل في شبكة مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر قبل استخدامه.

التكوين

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

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة الموضح في الرسم التخطيطي أدناه.



التكوينات

يستخدم هذا المستند التكوينات الموضحة أدناه.

- (Cisco 827 (CPE
- ضوء الموجه

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

(Cisco 827 (CPE
version 12.1 no service single-slot-reload-enable no service pad service timestamps debug uptime service timestamps log uptime no service password-encryption !

```
hostname 827
!
logging rate-limit console 10 except errors
!
ip subnet-zero
no ip finger
!
no ip dhcp-client network-discovery
vpdn enable

no vpdn logging
!
vpdn-group pppoe
request-dialin
protocol pppoe
!
!
!
crypto isakmp policy 20
encr 3des
authentication pre-share
group 2
crypto isakmp key sharedkey address 30.30.30.30
!
!
crypto ipsec transform-set dsltest esp-3des esp-md5-hmac
!
crypto map test 10 ipsec-isakmp
set peer 30.30.30.30
set transform-set dsltest
match address 101
!
interface Ethernet0
ip address 192.168.100.100 255.255.255.0
ip nat inside
!
interface ATM0
no ip address
no atm ilmi-keepalive
bundle-enable
dsl operating-mode ansi-dmt
!
interface ATM0.1 point-to-point
pvc 0/33
This is usually provided by the ISP. protocol pppoe ---!
pppoe-client dial-pool-number 1 ! ! interface Dialer1 ip
 address 20.20.20.20 255.255.255.0 !--- This is provided
by the ISP. !--- Another variation is ip address
.negotiated

ip mtu 1492
ip Nat outside
encapsulation ppp
no ip route-cache
no ip mroute-cache
dialer pool 1
ppp authentication chap callin
ppp chap hostname testuser
ppp chap password 7 00071A1507545A545C
crypto map test
!
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer1
no ip http server
```

```
!
ip Nat inside source route-map nonat interface Dialer1
                                                overload
          access-list 1 permit 192.168.100.0 0.0.0.255
     access-list 101 permit ip 192.168.100.0 0.0.0.255
                                   192.168.200.0 0.0.0.255
     access-list 105 deny   ip 192.168.100.0 0.0.0.255
                                   192.168.200.0 0.0.0.255
  access-list 105 permit ip 192.168.100.0 0.0.0.255 any
                                                        !
                                 route-map nonat permit 10
                                     match ip address 105
                                                        !
                                                        !
                                               line con 0
                                        transport input none
                                                  stopbits 1
                                              line vty 0 4
                                                    login
                                                        !
                                  scheduler max-task-time 5000
                                                      end
```

ضوء الموجه

```
                                                version 12.1
                                 no service single-slot-reload-enable
                                      service timestamps debug uptime
                                        service timestamps log uptime
                                       no service password-encryption
                                                        !
                                                hostname light
                                                        !
                          boot system flash:c3660-jk2s-mz.121-5.T8.bin
                                        logging buffered 4096 debugging
                           logging rate-limit console 10 except errors
                                                        !
                                                ip subnet-zero
                                                        !
                                                  no ip finger
                                                        !
                                                       ip cef
                                                        !
                                      crypto isakmp policy 20
                                                     encr 3des
                                    authentication pre-share
                                                     group 2
                    crypto isakmp key sharedkey address 20.20.20.20
                                                        !
crypto ipsec transform-set dsltest esp-3des esp-md5-hmac
                                                        !
                                    crypto map test 10 ipsec-isakmp
                                              set peer 20.20.20.20
                                   set transform-set dsltest
                                           match address 101
                                                        !
                                                call rsvp-sync
                                     cns event-service server
                                                        !
                                                        !
                                                        !
                                          controller E1 2/0
                                                        !
```

```
!
interface FastEthernet0/0
ip address 192.168.200.200 255.255.255.0
ip Nat inside
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 30.30.30.30 255.255.255.0
ip Nat outside
duplex auto
speed auto
crypto map test
!
interface Serial1/0
no ip address
shutdown
!
interface Serial1/1
no ip address
shutdown
!
interface Serial1/2
no ip address
shutdown
!
interface Serial1/3
no ip address
shutdown
!
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
!
ip kerberos source-interface any
ip Nat inside source route-map nonat interface
FastEthernet0/1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 30.30.30.1
ip http server
!
access-list 101 permit ip 192.168.200.0 0.0.0.255
192.168.100.0 0.0.0.255
access-list 105 deny   ip 192.168.200.0 0.0.0.255
192.168.100.0 0.0.0.255
access-list 105 permit ip 192.168.200.0 0.0.0.255 any
!
route-map nonat permit 10
match ip address 105
!
!
dial-peer cor custom
```

```
!
!
line con 0
exec-timeout 0 0
transport input none
line 97 108
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**.

ملاحظة: لفهم ما تشير إليه أوامر **العرض** التالية بدقة، يرجى الرجوع إلى أستكشاف أخطاء أمان IP وإصلاحها - فهم أوامر تصحيح الأخطاء واستخدامها.

- **show crypto isakmp sa** - يعرض اقتران أمان بروتوكول إدارة اقتران أمان الإنترنت (SA) (ISAKMP) الذي تم إنشاؤه بين النظراء.
- **show crypto ipSec** - يعرض IPSec SA الذي تم إنشاؤه بين الأقران.
- **show crypto engine connections active** - يعرض كل مرحلة 2 SA بنيت ومقدار حركة المرور المرسلة.

أمر العرض الجيد Router IPSec

- Cisco 827 (CPE **show crypto isakmp sa**)ضوء الموجه
- Cisco 827 (CPE **show crypto engine connections active**)ضوء الموجه
- **show crypto ipsec sa**

```
827#show crypto ipsec sa

interface: Dialer1
Crypto map tag: test, local addr. 20.20.20.20

(local ident (addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0
(remote ident (addr/mask/prot/port): (192.168.200.0/255.255.255.0/0/0
current_peer: 30.30.30.30
{,PERMIT, flags={origin_is_acl
pkts encaps: 208, #pkts encrypt: 208, #pkts digest 208#
pkts decaps: 208, #pkts decrypt: 208, #pkts verify 208#
pkts compressed: 0, #pkts decompressed: 0#
pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0#
send errors 2, #recv errors 0#

local crypto endpt.: 20.20.20.20, remote crypto endpt.: 30.30.30.30
path mtu 1500, media mtu 1500
current outbound spi: 4FE59EF2

:inbound esp sas
(spi: 0x3491ACD6(881962198
, transform: esp-3des esp-md5-hmac
```

{ ,in use settings ={Tunnel
slot: 0, conn id: 2000, flow_id: 1, crypto map: test
(sa timing: remaining key lifetime (k/sec): (4607840/3301
IV size: 8 bytes
replay detection support: Y

:inbound ah sas

:inbound pcp sas

:outbound esp sas
(spi: 0x4FE59EF2(1340448498
, transform: esp-3des esp-md5-hmac
{ ,in use settings ={Tunnel
slot: 0, conn id: 2001, flow_id: 2, crypto map: test
(sa timing: remaining key lifetime (k/sec): (4607837/3301
IV size: 8 bytes
replay detection support: Y

:outbound ah sas

:outbound pcp sas

interface: Virtual-Access1
Crypto map tag: test, local addr. 20.20.20.20

(local ident (addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0
(remote ident (addr/mask/prot/port): (192.168.200.0/255.255.255.0/0/0
current_peer: 30.30.30.30
{,PERMIT, flags={origin_is_acl
pkts encaps: 208, #**pkts encrypt: 208**, #**pkts digest 208**#
pkts decaps: 208, #**pkts decrypt: 208**, #**pkts verify 208**#
pkts compressed: 0, #**pkts decompressed: 0**#
pkts not compressed: 0, #**pkts compr. failed: 0**, #**pkts decompress failed: 0**#
send errors 2, #**recv errors 0**#

local crypto endpt.: 20.20.20.20, remote crypto endpt.: 30.30.30.30
path mtu 1500, media mtu 1500
current outbound spi: 4FE59EF2

:inbound esp sas
(spi: 0x3491ACD6(881962198
, transform: esp-3des esp-md5-hmac
{ ,in use settings ={Tunnel
slot: 0, conn id: 2000, flow_id: 1, crypto map: test
(sa timing: remaining key lifetime (k/sec): (4607840/3301
IV size: 8 bytes
replay detection support: Y

:inbound ah sas

:inbound pcp sas

:outbound esp sas
(spi: 0x4FE59EF2(1340448498
, transform: esp-3des esp-md5-hmac
{ ,in use settings ={Tunnel
slot: 0, conn id: 2001, flow_id: 2, crypto map: test
(sa timing: remaining key lifetime (k/sec): (4607837/3301
IV size: 8 bytes
replay detection support: Y

:outbound ah sas

```
:outbound pcp sas
```

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 حول أوامر تصحيح الأخطاء واستكشاف أخطاء أمان IP وإصلاحها - فهم أوامر تصحيح الأخطاء واستخدامها.

- **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.
- **ping** - يعرض الاتصال من خلال نفق VPN ويمكن إستخدامه بالاقتران مع أوامر **debug** و**show**.

```
827#ping
:[Protocol [ip
Target IP address: 192.168.200.200
Repeat count [5]: 100
Datagram size [100]: 1600
:[Timeout in seconds [2
Extended commands [n]: y
Source address or interface: 192.168.100.100
:[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 100, 1600-byte ICMP Echos to 192.168.200.200, timeout is 2 seconds
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 264/266/276 ms
```

معلومات ذات صلة

- صفحات دعم IPSec
- صفحات دعم توجيه IP
- مقدمة عن تشفير IPSec
- أستكشاف أخطاء الموجه Cisco 827 وإصلاحها
- 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).