EzVPN في وضع NEM مع الاتصال النفقي IOS موجه تكوين مثال على المنقسم

المحتويات

المقدمة

يوضح هذا التكوين الميزة الجديدة في الإصدار T(11)12.3 من برنامج Cisco IOS®Software التي تتيح لك تكوين موجه كعميل EZvpn والخادم على الواجهة نفسها. يمكن توجيه حركة مرور البيانات من عميل شبكة VPN إلى خادم EzVPN، ثم العودة إلى خادم EzVPN بعيد آخر.

ارجع إلى تكوين نظير شبكة LAN إلى شبكة LAN الديناميكية لموجه IPsec وعملاء شبكة VPN الديناميكي لمعرفة المزيد حول السيناريو الذي يوجد به تكوين شبكة LAN إلى شبكة LAN بين موجهات في بيئة موجهات باستخدام شبكة VPN من Cisco كما يتصل عملاء شبكة VPN من Cisco بالموجه ويتم إستخدام المصادقة الموسعة (Xauth).

للحصول على نموذج تكوين على EzVPN بين موجه Cisco 871 وموجه Cisco 7200VXR مع وضع NEM، ارجع إلى خادم Easy VPN 7200 إلى مثال التكوين عن بعد ل Easy VPN 871.

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 T(11)12.3 من Cisco على عميل EzVPN وموجه الخادم.
- برنامج IOS الإصدار (6)12.3 من Cisco على موجه خادم EzVPN البعيد (يمكن أن يكون هذا أي إصدار تشفير

يدعم ميزة خادم EzVPN).
- عميل شبكة VPN من Cisco، الإصدار x.4

ملاحظة: تمت إعادة تصنيف هذا المستند باستخدام موجه Cisco 3640 مع برنامج Cisco IOS، الإصدار 12.4(8).

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.

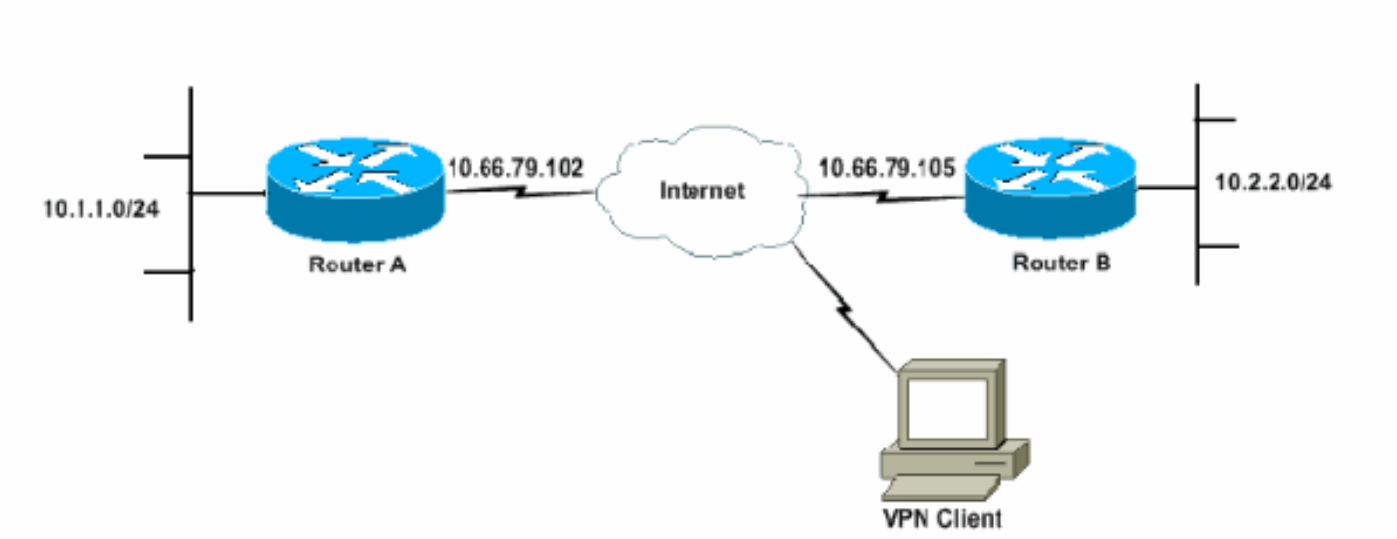
التكوين

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

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

الرسم التخطيطي للشبكة

في الرسم التخطيطي للشبكة هذا، يتم تكوين RouterA كعميل EzVPN وخادم على حد سواء. وهذا يسمح له بقبول الاتصالات من عملاء شبكة VPN، والعمل كعميل EzVPN عند إتصاله بموجه RouterB. يمكن توجيه حركة مرور البيانات من عميل الشبكة الخاصة الظاهرية (VPN) إلى الشبكات الموجودة خلف الموجه A والموجه B.



التكوينات

يجب تكوين الموجه A باستخدام ملفات تعريف IPsec لاتصالات عميل VPN. لا يعمل إستخدام تكوين خادم EZvpn قياسي على هذا الموجه مع تكوين عميل EzVPN. يفشل الموجه في تفاوض المرحلة 1.

في نموذج التكوين هذا، يرسل RouterB قائمة النفق المقسم 8/10.0.0.0 إلى RouterA. مع هذا تشكيل، ال VPN زبون بركة يستطيع لا يكون أي شيء في ال x.x.x.10 سوبر net. ما يحدث هو أن RouterA يقوم بإنشاء SA إلى RouterB لحركة المرور من 24/10.1.1.0 إلى 8/10.0.0.0. على سبيل المثال، لنفترض أن لديك اتصال عميل شبكة VPN وتحصل على عنوان IP من تجمع محلي بقيمة 10.3.3.1. يقوم الموجه A بإنشاء SA آخر لحركة المرور من

24/10.1.1.0 إلى 32/10.3.3.1 بنجاح. ومع ذلك، عند الرد على الحزم من عميل الشبكة الخاصة الظاهرية (VPN) ثم الضغط على RouterA، يرسلها الموجه A عبر النفق إلى RouterB. وذلك لأنها تطابق شبكة منطقة التخزين (SA) الخاصة بها والتي تبلغ 24/10.1.1.0 إلى 8/10.0.0.0 بدلا من المطابقة الأكثر تحديدا التي تبلغ 32/10.3.3.1.

أنت ينبغي أيضا شكلت انقسام tunneling على RouterB. وإلا، فلن تعمل حركة مرور عميل شبكة VPN أبدا. إذا لم يكن لديك تقسيم نفقي محدد (قائمة التحكم في الوصول (ACL 150) على RouterB في هذا المثال)، سيقوم RouterA بإنشاء SA لحركة المرور من 24/10.1.1.0 إلى 0/0.0.0.0 (جميع حركة المرور). عندما يربط عميل VPN أي عنوان IP ويستلم منه من أي تجمع، يتم إرسال حركة مرور الإرجاع إليه دائما عبر النفق إلى RouterB. ذلك لأنه يحصل على تطابق في البداية. بما أن SA هذا يعرف "كل حركة مرور"، لا يهم ما هو عنوان تجمع عناوين عميل VPN الخاص بك، فإن حركة المرور لا تعود إليه.

في الملخص، أنت ينبغي استعملت شق-tunneling، وال VPN عنوان بركة ك ينبغي كنت مختلف سوبر net من أي شبكة في ال split-tunnel قائمة.

يستخدم هذا المستند التكوينات التالية:

- الموجه A
- الموجه B

الموجه A

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname RouterA
!
boot-start-marker
boot-end-marker
!
logging buffered 4096 debugging
enable password cisco
!
username glenn password 0 cisco123
no network-clock-participate slot 1
no network-clock-participate wic 0
aaa new-model
!
!
aaa authentication login userlist local
aaa authorization network groupauthor local
aaa session-id common
ip subnet-zero
ip cef
!
ip dhcp-server 172.17.81.127
!
!
crypto isakmp policy 1
encr 3des
authentication pre-share
group 2
!
crypto isakmp keepalive 20 10
!
Group definition for the EzVPN server feature. !--- ---!
VPN Clients that connect in need to be defined with this
!--- group name/password and are allocated these
```

```
attributes. crypto isakmp client configuration group
                                        VPNCLIENTGROUP
                                           key mnbvcxz
                                    domain nuplex.com.au
                                          pool vpn1
                                           acl 150
                                                !
                                                !
IPsec profile for VPN Clients. crypto isakmp ---!
                                      profile VPNclient
                          description VPN clients profile
                      match identity group VPNCLIENTGROUP
                      client authentication list userlist
                    isakmp authorization list groupauthor
                     client configuration address respond
                                                !
                                                !
crypto ipsec transform-set 3des esp-3des esp-sha-hmac
                                                !
                                                !
Configuration for EzVPN Client configuration. These ---!
parameters !--- are configured on RouterB. ACL 120 is
the new "multiple-subnet" !--- feature of EzVPN. This
 allows the router to build an additional !--- SA for
traffic that matches the line in ACL 120 so that traffic
!--- from VPN Clients are routed over the EzVPN Client
tunnel !--- to RouterB. Without this, VPN Clients are
only able to !--- connect to subnets behind RouterA, and
                                                .not RouterB
                          crypto ipsec client ezvpn china
                                             connect auto
                                group china key mnbvcxz
                                mode network-extension
                                     peer 10.66.79.105
                                              acl 120
                                                !
                                                !


                         crypto dynamic-map SDM_CMAP_1 99
                                    set transform-set 3des
                               set isakmp-profile VPNclient
                                             reverse-route
                                                !
                                                !
crypto map SDM_CMAP_1 99 ipsec-isakmp dynamic SDM_CMAP_1
                                                !
                                                !
                                                !
                                  interface FastEthernet0/0
                                 description Outside interface
                       ip address 10.66.79.102 255.255.255.224
                                           ip nat outside
                                  ip virtual-reassembly
                                            duplex auto
                                             speed auto
                                    crypto map SDM_CMAP_1
                           crypto ipsec client ezvpn china
                                                !
                                                !
                                  interface FastEthernet1/0
                                 description Inside interface
                            ip address 10.1.1.1 255.255.255.0
                                           ip nat inside
                                  ip virtual-reassembly
```

```
                                                duplex auto
                                                 speed auto
                                 crypto ipsec client ezvpn china inside
                                                          !
                                                          !
  IP pool of addresses. Note that this pool must be ---!
!--- a different supernet to any of the split tunnel !--
   - networks sent down from RouterB. ip local pool vpn1
                                        192.168.1.1 192.168.1.254
                                                    ip classless
                                ip route 0.0.0.0 0.0.0.0 10.66.79.97
                                                          !
                                                 no ip http server
                                             no ip http secure-server
 ip nat inside source list 100 interface FastEthernet0/0
                                                        overload
                                                          !
access-list 100 deny   ip 10.1.1.0 0.0.0.255 192.168.1.0
                                                      0.0.0.255
        access-list 100 permit ip 10.1.1.0 0.0.0.255 any

Access-list that defines additional SAs for this !- ---!
        -- router to create to the head-end EzVPN server
 (RouterB). !--- Without this, RouterA only builds an SA
 for traffic !--- from 10.1.1.0 to 10.2.2.0. VPN Clients
  !--- that connect (and get a 192.168.1.0 address) !---
 are not able to get to 10.2.2.0. access-list 120 permit
        ip 192.168.1.0 0.0.0.255 10.0.0.0 0.255.255.255

  Split tunnel access-list for VPN Clients. access- ---!
                list 150 permit ip 10.1.1.0 0.0.0.255 any
        access-list 150 permit ip 10.2.2.0 0.0.0.255 any
                            dialer-list 1 protocol ip permit
                                                          !
                                                          !
                                                control-plane
                                                          !
                                                          !
                                                          !
                                                          !
                                                  line con 0
                                               exec-timeout 0 0
                                      login authentication nada
                                                  line aux 0
                                                 modem InOut
                          modem autoconfigure type usr_courier
                                             transport input all
                                                     speed 38400
                                                     line vty 0 4
                                          transport preferred all
                                              transport input all
                                                          !
                                                          !
                                                        end
```

الموجه B

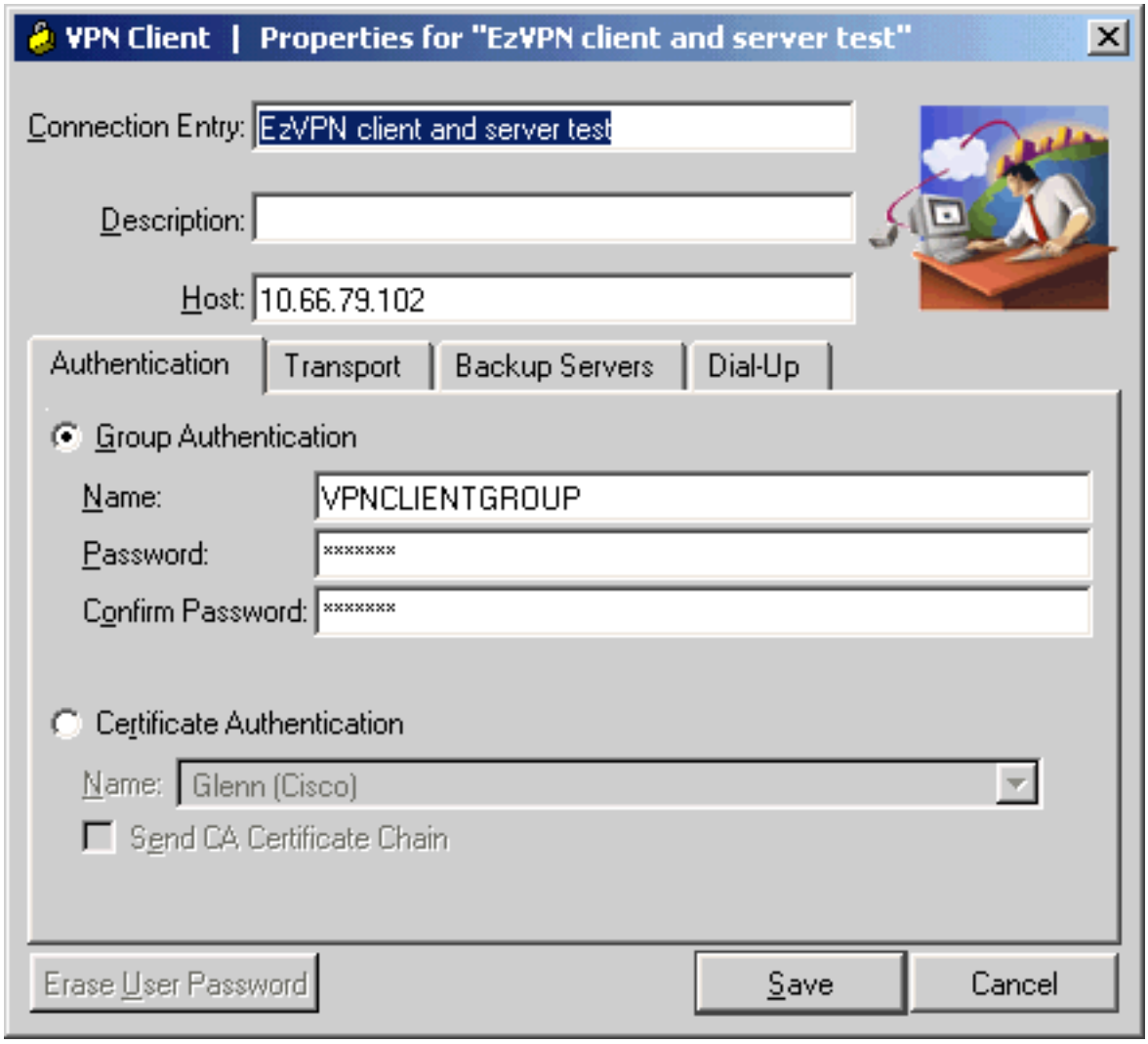
```
                                                version 12.4
                                service timestamps debug datetime msec
                                  service timestamps log datetime msec
                                       no service password-encryption
                                                          !
                                                hostname RouterB
```

```
!
boot-start-marker
boot-end-marker
!
logging buffered 4096 debugging
!
aaa new-model
!
!
No XAuth is defined but can be if needed. aaa ---!
authorization network groupauthor local
aaa session-id common
ip subnet-zero
ip cef
!
!
!
crypto isakmp policy 1
encr 3des
authentication pre-share
group 2
crypto isakmp keepalive 10
!
!
Standard EzVPN server configuration, !--- matching ---!
parameters defined on RouterA. crypto isakmp client
configuration group china
key mnbvcxz
acl 150
!
!
crypto ipsec transform-set 3des esp-3des esp-sha-hmac
!
crypto dynamic-map dynmap 1
set transform-set 3des
reverse-route
!
!
!
crypto map mymap isakmp authorization list groupauthor
crypto map mymap client configuration address respond
crypto map mymap 10 ipsec-isakmp dynamic dynmap
!
!
!
!
interface Ethernet0/0
description Outside interface
ip address 10.66.79.105 255.255.255.224
half-duplex
crypto map mymap
!
!
interface Ethernet0/1
description Inside interface
ip address 10.2.2.1 255.255.255.0
half-duplex
!
no ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 10.66.79.97
!
!
```

```
access-list 150 permit ip 10.0.0.0 0.255.255.255 any
!
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
!
!
!
end
```

تكوين عميل شبكة VPN

قم بإنشاء إدخال اتصال جديد يشير إلى عنوان IP الخاص بالموجه RouterA. اسم المجموعة في هذا المثال هو "vpnclientgroup" وكلمة المرور هي "mnbvcxz" كما يمكن رؤيتها في تكوين الموجه.



التحقق من الصحة واستكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك إستخدامها للتأكد من أن التكوين يعمل بشكل صحيح. راجع أستكشاف أخطاء أمان IP وإصلاحها - فهم أوامر تصحيح الأخطاء واستخدامها للحصول على معلومات إضافية للتحقق/أستكشاف الأخطاء وإصلاحها. إن يصادف أنت أي VPN زبون إصدار أو خطأ، أحلت ال VPN زبون GUI خطأ أداة بحث.

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

معلومات ذات صلة

- تكوين ملف تعريف IPsec
- صفحة دعم عميل شبكة VPN من Cisco
- صفحة دعم 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).