

نيوكت عم ة دراو لا ة قدا صم لا ليك و ة قدا صم و NAT ة يامح راج مادخت ساب VPN و IPsec لي مع Cisco IOS

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [الاصطلاحات](#)
- [التكوين](#)
- [الرسم التخطيطي للشبكة](#)
- [التكوينات](#)
- [التحقق من الصحة](#)
- [استكشاف الأخطاء وإصلاحها](#)
- [معلومات ذات صلة](#)

المقدمة

يتيح هذا التكوين العينة لعميل الشبكة الخاصة الظاهرية (VPN) الوصول إلى خادم على شبكة أخرى من خلال نفق IPsec، بعد نجاح مصادقة المستخدم.

يجمع جهاز الكمبيوتر 99.99.99.5 مستعرض الويب للوصول إلى المحتوى الموجود على الخادم على 10.13.1.98. بما أن عميل VPN على الكمبيوتر الشخصي تم تكوينه للانتقال من خلال نقطة نهاية النفق 99.99.99.1 للوصول إلى شبكة 10.13.1.x، تم إنشاء نفق IPsec وبحصل الكمبيوتر على عنوان IP من التجمع المسمى "ourpool" (بما أنك تقوم بتكوين الوضع). يطلب الموجه 3640 المصادقة. بعد أن يدخل المستخدم اسم مستخدم وكلمة مرور (مخزنا على خادم TACACS+ في 172.18.124.97)، تتم إضافة قائمة الوصول التي تم تمريرها من الخادم إلى قائمة الوصول 117.

ملاحظة: تم إدخال الأمر ip auth-proxy في البرنامج Cisco IOS® Software، الإصدار T.12.0.5.

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.12.0.7 من Cisco
- الموجه (Cisco 3640 (c3640-jo3s56i-mz.121-2.3.T
- Cisco Secure VPN Client 1.0 (يظهر على هيئة 2.0.7 في قائمة تعليمات عميل (IR > About أو Cisco Secure VPN Client 1.1 (يظهر على هيئة 2.1.12 في قائمة تعليمات عميل (IRE > About
- 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

راجع [اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.](#)

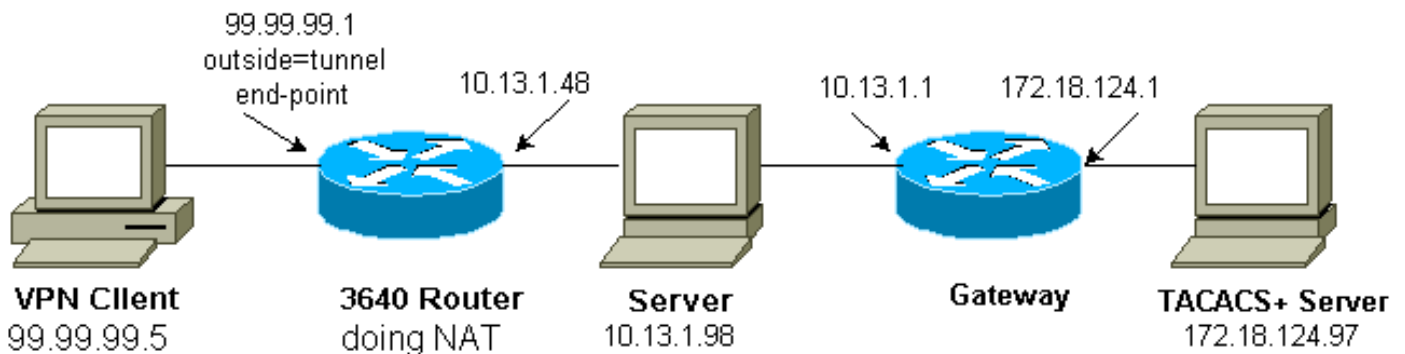
التكوين

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

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

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



التكوينات

يستعمل هذا وثيقة هذا تشكيل:

```

Cisco 3640 الموجه تكوين
:Current configuration
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname carter
!
aaa new-model
aaa authentication login default group tacacs+ none
aaa authorization exec default group tacacs+ none
+aaa authorization auth-proxy default group tacacs

```

```

enable secret 5 $1$cSvL$F6VxA7kBFAGHvhBbRlNS20
enable password ww
!
ip subnet-zero
!
ip inspect name myfw cuseeme timeout 3600
ip inspect name myfw ftp timeout 3600
ip inspect name myfw http timeout 3600
ip inspect name myfw rcmd timeout 3600
ip inspect name myfw realaudio timeout 3600
ip inspect name myfw smtp timeout 3600
ip inspect name myfw sqlnet timeout 3600
ip inspect name myfw streamworks timeout 3600
ip inspect name myfw tftp timeout 30
ip inspect name myfw udp timeout 15
ip inspect name myfw tcp timeout 3600
ip inspect name myfw vdolive
ip auth-proxy auth-proxy-banner
ip auth-proxy auth-cache-time 10
ip auth-proxy name list_a http
ip audit notify log
ip audit po max-events 100
cns event-service server
!
crypto isakmp policy 10
hash md5
authentication pre-share
crypto isakmp key cisco1234 address 0.0.0.0 0.0.0.0
crypto isakmp client configuration address-pool local
ourpool
!
crypto ipsec transform-set mypolicy esp-des esp-md5-hmac
!
crypto dynamic-map dyna 10
set transform-set mypolicy
!
crypto map test client configuration address initiate
crypto map test client configuration address respond
crypto map test 5 ipsec-isakmp dynamic dyna
!
interface Loopback0
ip address 1.1.1.1 255.255.255.0
!
interface Ethernet0/0
ip address 10.13.1.48 255.255.255.0
ip nat inside
ip inspect myfw in
ip route-cache policy
no ip mroute-cache
ip policy route-map nonat
no mop enabled
!
interface TokenRing0/0
no ip address
shutdown
ring-speed 16
!
interface Ethernet2/0
ip address 99.99.99.1 255.255.255.0
ip access-group 117 in
ip nat outside
ip auth-proxy list_a
no ip route-cache
no ip mroute-cache

```

```

no mop enabled
crypto map test
!
interface TokenRing2/0
no ip address
shutdown
ring-speed 16
!
ip local pool ourpool 10.2.1.1 10.2.1.254
ip nat pool outsidepool 99.99.99.50 99.99.99.60 netmask
255.255.255.0
ip nat inside source route-map rmap pool outsidepool
ip classless
ip route 0.0.0.0 0.0.0.0 99.99.99.20
ip route 172.18.124.0 255.255.255.0 10.13.1.1
no ip http server
!
access-list 110 deny ip 10.13.1.0 0.0.0.255 10.2.1.0
0.0.0.255
access-list 110 permit ip 10.13.1.0 0.0.0.255 any
access-list 117 permit esp any any
access-list 117 permit udp any any eq isakmp
access-list 120 permit ip 10.13.1.0 0.0.0.255 10.2.1.0
0.0.0.255
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
route-map rmap permit 10
match ip address 110
!
route-map nonat permit 10
match ip address 120
set ip next-hop 1.1.1.2
!
route-map nonat permit 20
!
tacacs-server host 172.18.124.97
tacacs-server key cisco
!
line con 0
transport input none
line aux 0
line vty 0 4
password ww
!
end

```

التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

ارجع إلى [وكيل مصادقة أكتشاف الأخطاء وإصلاحها](#) للحصول على معلومات حول أكتشاف الأخطاء وإصلاحها.

ملاحظة: ارجع إلى [معلومات مهمة حول أوامر التصحيح](#) قبل استخدام أوامر debug.

معلومات ذات صلة

- [عمل شبكة VPN من Cisco](#)
- [مفاوضة IPsec/بروتوكولات IKE](#)
- [الدعم الفني لجدار حماية Cisco IOS](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

