تكوين جدار حماية PIX وعملاء VPN باستخدام IPSec و MPPE و PPTP

المحتويات

المقدمة

في هذا التكوين النموذجي، تقوم أربعة أنواع مختلفة من العملاء بتوصيل حركة مرور البيانات وتشفيرها باستخدام جدار حماية PIX الآمن من Cisco كنقطة نهاية للنفق:

- المستخدمون الذين يقومون بتشغيل Cisco Secure VPN Client 1.1 على Microsoft Windows 95/98/NT
- المستخدمون الذين يقومون بتشغيل Cisco Secure VPN 3000 Client 2.5.x على Windows 95/98/NT
- المستخدمون الذين يقومون بتشغيل عملاء بروتوكول الاتصال النفقي من نقطة إلى نقطة (PPTP) لنظام التشغيل Windows 98/2000/XP
- المستخدمون الذين يقومون بتشغيل عميل Cisco VPN 3.x/4.x على Windows 95/98/NT/2000/XP

في هذا المثال، تم تكوين تجمع واحد ل IPsec و PPTP. ولكن يمكن أيضا جعل البرك منفصلة.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- برنامج PIX الإصدار 6.3.3
- Cisco Secure VPN Client 1.1
- Cisco VPN 3000 Client، الإصدار 2.5
- عميل شبكة VPN من Cisco الإصداران x.3 و x.4
- عملاء Microsoft Windows 2000 و Windows 98

ملاحظة: تم إختبار ذلك على برنامج PIX الإصدار 6.3.3 ولكن ينبغي العمل على الإصدار x.5.2 و 5.3.1. برنامج PIX الإصدار x.6 مطلوب ل Cisco VPN Client الإصدار x.3 و x.4. (تتم إضافة الدعم ل Cisco VPN 3000 Client 2.5 في برنامج PIX الإصدار x.5.2. يعمل التكوين أيضا لبرنامج PIX الإصدار x.5.1، باستثناء جزء عميل Cisco VPN 3000.) يجب إجراء IPsec و MPPE (PPTP/Microsoft Point-to-Point Encryption) للعمل بشكل منفصل أولا. إذا لم تعمل بشكل منفصل، فإنها لا تعمل معا.

ملاحظة: يستخدم PIX 7.0 الأمر **فحص RPC** لمعالجة حزم RPC. يمكن الأمر فحص SunRPC فحص التطبيقات لبروتوكول Sun RPC أو يعطله. يمكن تشغيل خدمات RPC من Sun على أي منفذ على النظام. عند محاولة أحد العملاء الوصول إلى خدمة RPC على خادم، يجب عليه معرفة المنفذ الذي تعمل عليه هذه الخدمة المحددة. وذلك من خلال الاستعلام عن عملية PortMapper على المنفذ رقم 111 المعروف. يرسل العميل رقم برنامج RPC الخاص بالخدمة، ويستعيد رقم المنفذ. من هذه النقطة، يرسل برنامج العميل استعلامات RPC الخاصة به إلى ذلك المنفذ الجديد.

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.

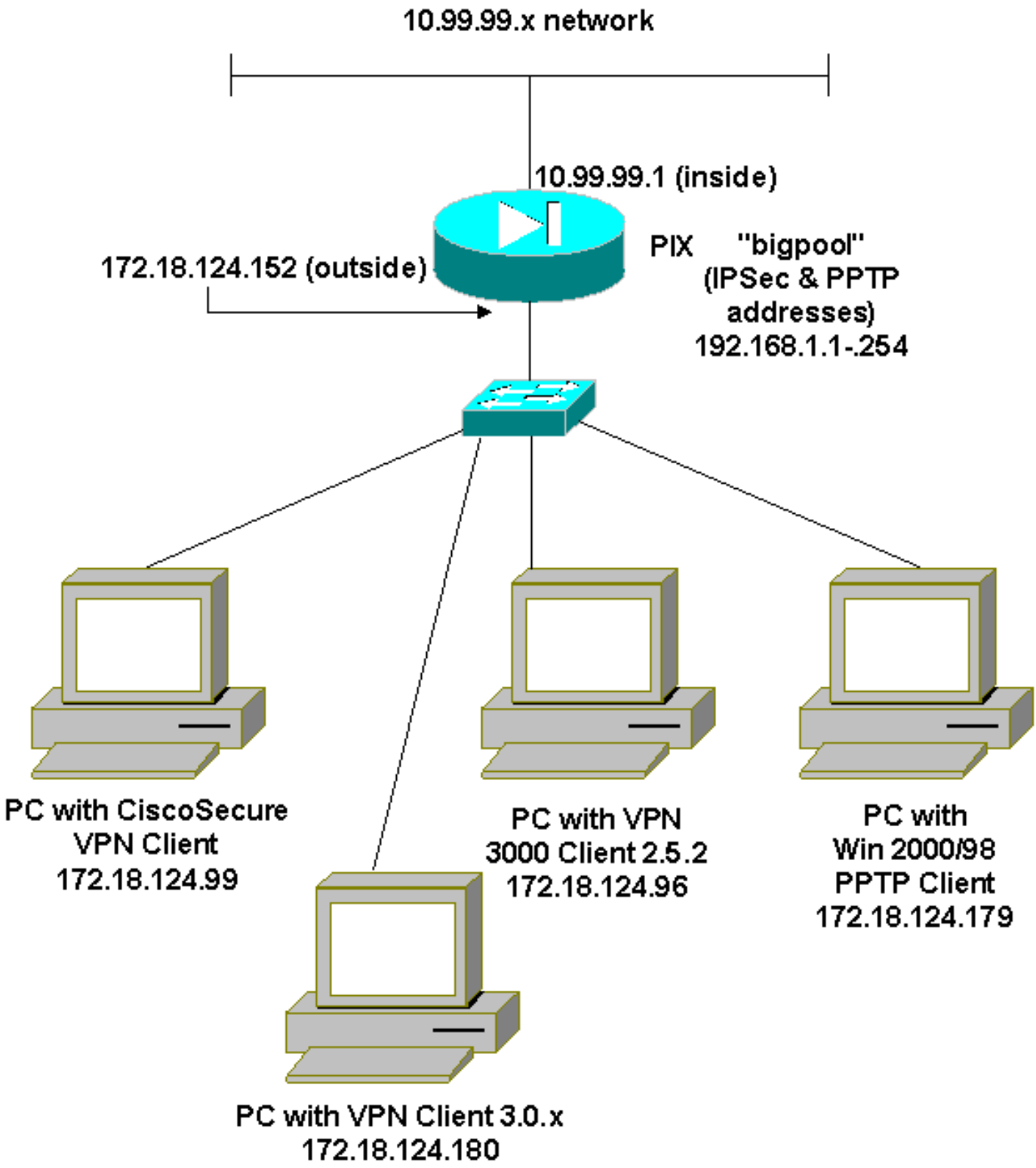
التكوين

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

يستخدم هذا المستند إعداد الشبكة الموضح في هذا الرسم التخطيطي.



التكوينات

يستخدم هذا المستند هذه التكوينات.

- جدار حماية PIX الآمن من Cisco
- Cisco Secure VPN Client 1.1

جدار حماية PIX الآمن من Cisco
(PIX Version 6.3(3 interface ethernet0 auto

```
                                interface ethernet1 100full
                            nameif ethernet0 outside security0
                          nameif ethernet1 inside security100
                 enable password 8Ry2YjIyt7RRXU24 encrypted
                           passwd 2KFQnbNIdI.2KYOU encrypted
                                        hostname goss-515A
                                   fixup protocol ftp 21
                              fixup protocol h323 h225 1720
                           fixup protocol h323 ras 1718-1719
                                   fixup protocol http 80
                                   fixup protocol ils 389
                                   fixup protocol rsh 514
                                  fixup protocol rtsp 554
                                  fixup protocol sip 5060
                               fixup protocol sip udp 5060
                                fixup protocol skinny 2000
                                   fixup protocol smtp 25
                                fixup protocol sqlnet 1521
                                                    names
          access-list 101 permit ip 10.99.99.0 255.255.255.0
                                  192.168.1.0 255.255.255.0
                                               pager lines 24
                                             mtu outside 1500
                                              mtu inside 1500
            ip address outside 172.18.124.152 255.255.255.0
                 ip address inside 10.99.99.1 255.255.255.0
                                 ip audit info action alarm
                              ip audit attack action alarm
          ip local pool bigpool 192.168.1.1-192.168.1.254
                                           pdm history enable
                                            arp timeout 14400
                              nat (inside) 0 access-list 101
                                        timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
                                         0:10:00 h225 1:00:00
 timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media
                                                  0:02:00
                             timeout uauth 0:05:00 absolute
                        +aaa-server TACACS+ protocol tacacs
                          aaa-server RADIUS protocol radius
                            aaa-server LOCAL protocol local
                                    no snmp-server location
                                     no snmp-server contact
                                snmp-server community public
                                 no snmp-server enable traps
                                        floodguard enable
                               sysopt connection permit-ipsec
                               sysopt connection permit-pptp
    crypto ipsec transform-set myset esp-des esp-md5-hmac
     crypto dynamic-map dynmap 10 set transform-set myset
          crypto map mymap 10 ipsec-isakmp dynamic dynmap
   crypto map mymap client configuration address initiate
    crypto map mymap client configuration address respond
                        crypto map mymap interface outside
                                isakmp enable outside
     Cisco Secure_VPNClient_key. isakmp key ******** ---!
                              address 0.0.0.0 netmask 0.0.0.0
                                    isakmp identity address
  isakmp client configuration address-pool local bigpool
                                                  outside

        ISAKMP Policy for Cisco VPN Client 2.5 or !--- ---!
             Cisco Secure VPN Client 1.1. isakmp policy 10
                                  authentication pre-share
```

```
isakmp policy 10 encryption des
isakmp policy 10 hash md5

The 1.1 and 2.5 VPN Clients use Diffie-Hellman (D- ---!
H) !--- group 1 policy (PIX default). isakmp policy 10
group 1
isakmp policy 10 lifetime 86400

ISAKMP Policy for VPN Client 3.0 and 4.0. isakmp ---!
policy 20 authentication pre-share
isakmp policy 20 encryption des
isakmp policy 20 hash md5

The 3.0/4.0 VPN Clients use D-H group 2 policy !--- ---!
and PIX 6.0 code. isakmp policy 20 group 2
isakmp policy 20 lifetime 86400
vpngroup vpn3000-all address-pool bigpool
vpngroup vpn3000-all dns-server 10.99.99.99
vpngroup vpn3000-all wins-server 10.99.99.99
vpngroup vpn3000-all default-domain password
vpngroup vpn3000-all idle-time 1800

VPN 3000 group_name and group_password. vpngroup ---!
******** vpn3000-all password
telnet timeout 5
ssh timeout 5
console timeout 0
vpdn group 1 accept dialin pptp
vpdn group 1 ppp authentication pap
vpdn group 1 ppp authentication chap
vpdn group 1 ppp authentication mschap
vpdn group 1 ppp encryption mppe auto
vpdn group 1 client configuration address local bigpool
vpdn group 1 pptp echo 60
vpdn group 1 client authentication local

PPTP username and password. vpdn username cisco ---!
********* password
vpdn enable outside
terminal width 80
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
end :
#goss-515A
```

Cisco Secure VPN Client 1.1

```
TACconn 1-
My Identity
Connection security: Secure
Remote Party Identity and addressing
ID Type: IP subnet
10.99.99.0
255.255.255.0
Port all Protocol all

Connect using secure tunnel
ID Type: IP address
172.18.124.152

Pre-shared Key=CiscoSecure_VPNClient_key

(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
```

Cisco VPN 3000 Client 2.5.x أو Cisco VPN Client 3.x و x.4

حدد **خيارات** > **خصائص** > **مصادقة**. يتطابق اسم المجموعة وكلمة مرور المجموعة مع group_name و group_password على PIX كما في:

```
******** vpngroup vpn3000-all password
Host-name = 172.18.124.152
```

إعداد عميل Windows 98/2000/XP PPTP

يمكنك الاتصال بالمورد الذي يقوم بإنشاء عميل PPTP. راجع كيفية تكوين جدار حماية PIX الآمن من Cisco لاستخدام PPTP للحصول على معلومات حول كيفية إعداد هذا الإعداد.

التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها 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**.

تصحيح أخطاء PIX IPsec

- **debug crypto ipSec**—يعرض مفاوضات IPsec للمرحلة 2.
- **debug crypto isakmp**—يعرض مفاوضات بروتوكول إدارة المفاتيح وارتباط أمان الإنترنت (ISAKMP) للمرحلة الأولى.
- **debug crypto engine**—يعرض حركة مرور البيانات التي يتم تشفيرها.

تصحيح أخطاء PIX PPTP

- **debug ppp io**—يعرض معلومات الحزمة للواجهة الظاهرية PPTP PPP.
- **debug ppp خطأ**—يعرض رسائل خطأ الواجهة الظاهرية PPTP.
- **debug vpdn خطأ**—يعرض رسائل خطأ بروتوكول PPTP.
- **debug vpdn** packet—يعرض معلومات حزمة PPTP حول حركة مرور بيانات PPTP.
- **debug vpdn events**— يعرض معلومات تغيير حدث نفق PPTP.
- **debug ppp uauth**—يعرض رسائل تصحيح أخطاء مصادقة مستخدم AAA لواجهة PPTP الظاهرية PPP.

المشاكل ذات الصلة ب Microsoft

- كيفية الاحتفاظ باتصالات RAS نشطة بعد تسجيل الخروج —عند تسجيل الخروج من عميل "خدمة الوصول عن بعد إلى RAS) "Windows)، يتم قطع اتصال RAS تلقائيا. لتظل متصلا بعد تسجيل الخروج، قم بتمكين مفتاح KeepRasConnections في السجل على عميل RAS.
- لا يتم تنبيه المستخدم عند تسجيل الدخول باستخدام بيانات الاعتماد المخزنة مؤقتا —الأعراض - عند محاولة تسجيل الدخول إلى مجال من محطة عمل قائمة على نظام التشغيل Windows أو خادم عضو ولا يمكن تحديد موقع وحدة التحكم بالمجال، لا يتم عرض أية رسالة خطأ. وبدلا من ذلك، يتم تسجيل دخولك إلى الكمبيوتر المحلي باستخدام بيانات الاعتماد المخزنة مؤقتا.
- كيفية كتابة ملف LMHOSTS لمسائل التحقق من صحة المجال ودقة الأسماء الأخرى —يمكن أن تكون هناك حالات تشهد فيها مشاكل تحليل الاسم على شبكة TCP/IP لديك وتحتاج إلى إستخدام ملفات LmHosts لحل أسماء NetBIOS. تناقش هذه المقالة الطريقة المناسبة لإنشاء ملف LmHosts للمساعدة في تحليل الاسم والتحقق من صحة المجال.

معلومات ذات صلة

- صفحات دعم مفاوضة IPsec/بروتوكولات IKE
- مرجع أوامر PIX
- صفحة دعم أجهزة الأمان Cisco PIX 500 Series Security Appliances
- طلبات التعليقات (RFCs)
- تكوين أمان شبكة IPsec
- تكوين بروتوكول أمان Internet Key Exchange
- 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).