PIX: الوصول إلى PDM من واجهة خارجية عبر نفق VPN

المحتويات

المقدمة

يوثق هذا النموذج من التكوين كيفية تكوين نفق VPN من شبكة LAN إلى شبكة LAN باستخدام جدرتي حماية PIX. يتم تشغيل مدير أجهزة PIX (PDM) على PIX البعيد من خلال الواجهة الخارجية على الجانب العام ويقوم بتشفير كل من الشبكة العادية وحركة مرور PDM.

PDM هي أداة تكوين قائمة على المستعرض تم تصميمها لتساعدك في إعداد جدار حماية PIX لديك وتكوينه ومراقبته باستخدام واجهة المستخدم الرسومية (GUI). لا تحتاج إلى معرفة شاملة بواجهة سطر أوامر (CLI) جدار حماية PIX.

المتطلبات الأساسية

المتطلبات

يتطلب هذا المستند فهما أساسيا لتشفير IPsec و PDM.

تأكد من أن جميع الأجهزة المستخدمة في طبقتك تفي بالمتطلبات الموضحة في دليل تثبيت أجهزة جدار حماية Cisco PIX، الإصدار 6.3.

المكونات المستخدمة

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

- برنامج جدار حماية PIX الإصدار 6.3(1) و 6.3(3) من Cisco
- PIX A و PIX B هما Cisco PIX Firewall 515E
- يستخدم PIX B الإصدار 2.1(1) من PDM**ملاحظة:** لا يعمل PDM 3.0 مع إصدارات برامج جدار حماية PIX الأقدم من الإصدار 6.3. PDM الإصدار 3.0 هو صورة فردية تدعم فقط PIX Firewall الإصدار 6.3.**ملاحظة:** تفرض تكوينات NAT الخاصة بالسياسة 0 .3 PDM في وضع الشاشة. يتم دعم NAT الخاص بالنهج في الإصدار 4.0 من PDM والإصدارات الأحدث.**ملاحظة:** عندما يطلب منك اسم مستخدم وكلمة مرور ل PIX Device Manager (PDM)، فإن الإعدادات الافتراضية لا تتطلب اسم مستخدم. إن شكلت يمكن كلمة كان سابقا، دخلت أن كلمة بما أن ال PDM كلمة. إذا لم يكن هناك تمكين كلمة مرور، أترك كلا من إدخالات اسم المستخدم وكلمة المرور فارغة وانقر **موافق** للمتابعة.

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.

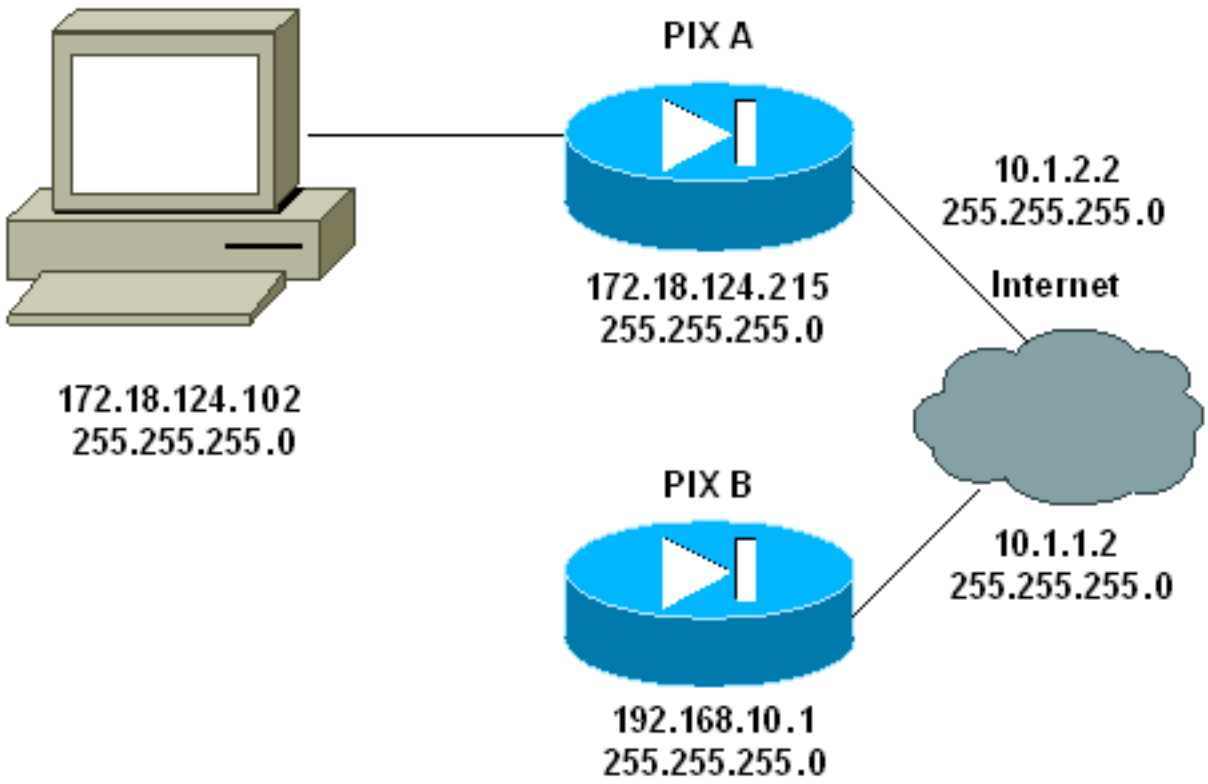
التكوين

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 التالي:



التكوينات

يستخدم هذا المستند التكوينات التالية:

- بيكس أي
- بي بي

بيكس أي

```
PIX A

(PIX Version 6.3(3
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIXA
domain-name cisco.com
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
Allow traffic from the host PC that is going to !-- ---!
- run the PDM to the outside interface of PIX B. access-
    list 101 permit ip host 172.18.124.102 host 10.1.1.2
Allow traffic from the private network behind PIX A ---!
!--- to access the private network behind PIX B. access-
          list 101 permit ip 172.18.124.0 255.255.255.0
                                    192.168.10.0 255.255.255.0
                                              pager lines 24
                                   interface ethernet0 10baset
                                   interface ethernet1 10baset
                                              mtu outside 1500
                                               mtu inside 1500
                        ip address outside 10.1.2.2 255.255.255.0
                  ip address inside 172.18.124.215 255.255.255.0
                                    ip audit info action alarm
                                ip audit attack action alarm
                                         pdm history enable
                                          arp timeout 14400
Do not use NAT !--- on traffic which matches access ---!
  control list (ACL) 101. nat (inside) 0 access-list 101
     Configures a default route towards the gateway ---!
        router. route outside 0.0.0.0 0.0.0.0 10.1.2.1 1
                                       timeout xlate 3:00:00
    timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
  rpc 0:10:00 h323 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
   Enable the HTTP server required to run PDM. http ---!
                                                server enable
   This is the interface name and IP address of the ---!
host or !--- network that initiates the HTTP connection.
                        http 172.18.124.102 255.255.255.255 inside
                                       no snmp-server location
```

```
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
Implicitly permit any packet that came from an ---!
    IPsec !--- tunnel and bypass the checking of an
  associated access-list, conduit, or !--- access-group
    command statement for IPsec connections. sysopt
                    connection permit-ipsec
Specify IPsec (phase 2) transform set. crypto ipsec ---!
                transform-set vpn esp-3des esp-md5-hmac
 Specify IPsec (phase 2) attributes. crypto map vpn ---!
                                    10 ipsec-isakmp
              crypto map vpn 10 match address 101
              crypto map vpn 10 set peer 10.1.1.2
            crypto map vpn 10 set transform-set vpn
                 crypto map vpn interface outside
 Specify ISAKMP (phase 1) attributes. isakmp enable ---!
                                          outside
        isakmp key ******** address 10.1.1.2 netmask
                                    255.255.255.255
                              isakmp identity address
          isakmp policy 10 authentication pre-share
                 isakmp policy 10 encryption 3des
                    isakmp policy 10 hash md5
                   isakmp policy 10 group 1
                isakmp policy 10 lifetime 86400
                                  telnet timeout 5
                                     ssh timeout 5
                                terminal width 80
Cryptochecksum:24e43efa87d6ef07dfabe097b82b5b40
                                              end :
                                             [OK]
                                    #(PIXA(config
```

بي بي

```
                                    PIX B
                                (PIX Version 6.3(1
                  nameif ethernet0 outside security0
                 nameif ethernet1 inside security100
          enable password 8Ry2YjIyt7RRXU24 encrypted
              passwd 2KFQnbNIdI.2KYOU encrypted
                                hostname PIXB
                            domain-name cisco.com
                             fixup protocol ftp 21
                           fixup protocol http 80P
                         fixup protocol h323 1720
                           fixup protocol rsh 514
                           fixup protocol smtp 25
                       fixup protocol sqlnet 1521
                          fixup protocol sip 5060
                       fixup protocol skinny 2000
                                         names
Allow traffic from the host PC that is going to !-- ---!
- run the PDM to the outside interface of PIX B. access-
    list 101 permit ip host 10.1.1.2 host 172.18.124.102
Allow traffic from the private network behind PIX A ---!
!--- to access the private network behind PIX B. access-
          list 101 permit ip 192.168.10.0 255.255.255.0
                      172.18.124.0 255.255.255.0
                                    pager lines 24
                  interface ethernet0 10baset
```

```
                                interface ethernet1 10baset
                                                mtu outside 1500
                                                 mtu inside 1500
                                ip address outside 10.1.1.2 255.255.255.0
                                ip address inside 192.168.10.1 255.255.255.0
                                                ip audit info action alarm
                                                ip audit attack action alarm
    Assists PDM with network topology discovery by ---!
    associating an external !--- network object with an
 interface. Note: The pdm location !--- command does not
                                .control which host can launch PDM

    pdm location 172.18.124.102 255.255.255.255 outside
                                                pdm history enable
                                                 arp timeout 14400
   Do not use NAT on traffic which matches ACL 101. ---!
                                nat (inside) 0 access-list 101
     Configures a default route towards the gateway ---!
        router. route outside 0.0.0.0 0.0.0.0 10.1.1.1 1
                                                timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
                                                             0:10:00
                h323 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
  Enables the HTTP server required to run PDM. http ---!
                                                server enable
   This is the interface name and IP address of the ---!
host or !--- network that initiates the HTTP connection.
                http 172.18.124.102 255.255.255.255 outside
                                              no snmp-server location
                                               no snmp-server contact
                                snmp-server community public
                                 no snmp-server enable traps
                                                floodguard enable
    Implicitly permit any packet that came from an ---!
        IPsec !--- tunnel and bypass the checking of an
   associated access-list, conduit, or !--- access-group
        command statement for IPsec connections. sysopt
                                                connection permit-ipsec
Specify IPsec (phase 2) transform set. crypto ipsec ---!
                                transform-set vpn esp-3des esp-md5-hmac
 Specify IPsec (phase 2) attributes. crypto map vpn ---!
                                                10 ipsec-isakmp
                                crypto map vpn 10 match address 101
                                crypto map vpn 10 set peer 10.1.2.2
                              crypto map vpn 10 set transform-set vpn
                                      crypto map vpn interface outside
                                              isakmp enable outside
    Specify ISAKMP (phase 1) attributes. isakmp key ---!
                ******** address 10.1.2.2 netmask 255.255.255.255
                          isakmp policy 10 authentication pre-share
                                  isakmp policy 10 encryption 3des
                                        isakmp policy 10 hash md5
                                         isakmp policy 10 group 1
                                isakmp policy 10 lifetime 86400
                                                telnet timeout 5
                                                   ssh timeout 5
                                                terminal width 80
        Cryptochecksum:d5ba4da0d610d0c6140e1b781abef9d0
                                                             end :
                                                             [OK]
                                                #(PIXB(config
```

التحقق من الصحة

يوفر هذا القسم معلومات يمكنك إستخدامها للتأكد من أن التكوين يعمل بشكل صحيح.

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

- show crypto isakmp sa/show isakmp sa —يتحقق من أن المرحلة 1 تؤسس.
- show crypto ipSec — يتحقق من أن المرحلة 2 تؤسس.
- show crypto engine — يعرض إحصائيات الاستخدام لمحرك التشفير الذي يستخدمه جدار الحماية.

ملخص الأوامر

ما إن وضعت VPN أمر داخل ال VPN، PIXs نفق ينبغي أسست عندما حركة مرور بين ال PDM pc (172.18.124.102 وال خارجي من (10.1.1.2 PIX B). عند هذه النقطة، يمكن لجهاز PDM pc الانتقال إلى https://10.1.1.2 والوصول إلى واجهة PDM الخاصة ب PIX B عبر نفق VPN.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها. راجع أستكشاف أخطاء مدير أجهزة PIX وإصلاحها لاستكشاف أخطاء PDM ذات الصلة وإصلاحها.

إخراج تصحيح الأخطاء للعينة

show crypto isakmp sa

يوضح هذا الإخراج نفقا تم تكوينه بين 10.1.1.2 و 10.1.2.2.

```
PIXA#show crypto isakmp sa
                                    Total     : 1
                                    Embryonic : 0
dst         src         state     pending    created
QM_IDLE        0           1    10.1.2.2    10.1.1.2
```

show crypto ipsec sa

يوضح هذا الإخراج نفقا يمر بحركة المرور بين 10.1.1.2 و 172.18.124.102.

```
PIXA#show crypto ipsec sa

                                    interface: outside
                        Crypto map tag: vpn, local addr. 10.1.2.2

(local  ident (addr/mask/prot/port): (172.18.124.102/255.255.255.255/0/0
      (remote ident (addr/mask/prot/port): (10.1.1.2/255.255.255.255/0/0
                                    current_peer: 10.1.1.2
                                    {,PERMIT, flags={origin_is_acl     <
      pkts encaps: 14472, #pkts encrypt: 14472, #pkts digest 14472#
      pkts decaps: 16931, #pkts decrypt: 16931, #pkts verify 16931#
                          pkts compressed: 0, #pkts decompressed: 0#
                  ,pkts not compressed: 0, #pkts compr. failed: 0#
```

```
    pkts decompress failed: 0, #send errors 9, #recv errors 0#

local crypto endpt.: 10.1.2.2, remote crypto endpt.: 10.1.1.2
             path mtu 1500, ipsec overhead 56, media mtu 1500
                           current outbound spi: 4acd5c2a

                                        :inbound esp sas
                                  (spi: 0xcff9696a(3489229162
                        , transform: esp-3des esp-md5-hmac
                                { ,in use settings ={Tunnel
                      slot: 0, conn id: 2, crypto map: vpn
(sa timing: remaining key lifetime (k/sec): (4600238/15069
                                        IV size: 8 bytes
                                replay detection support: Y

                                         :inbound ah sas

                                         :inbound pcp sas

                                        :outbound esp sas
                                  (spi: 0x4acd5c2a(1254972458
                        , transform: esp-3des esp-md5-hmac
                                { ,in use settings ={Tunnel
                      slot: 0, conn id: 1, crypto map: vpn
(sa timing: remaining key lifetime (k/sec): (4607562/15069
                                        IV size: 8 bytes
                                replay detection support: Y

                                         :outbound ah sas

                                         :outbound pcp sas
```

معلومات ذات صلة

- مرجع أوامر PIX
- أجهزة الأمان Cisco PIX 500 Series Security Appliances
- طلبات التعليقات (RFCs)
- 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).