تكوين نفق IPSec LAN إلى LAN بين جدار حماية Cisco PIX وجدار حماية NetScreen

المحتويات

المقدمة

يصف هذا المستند الإجراء اللازم المستخدم لإنشاء نفق IPsec من شبكة LAN بين جدار حماية Cisco PIX وجدار حماية NetScreen باستخدام أحدث البرامج. توجد شبكة خاصة خلف كل جهاز تتصل بجدار الحماية الآخر من خلال نفق IPsec.

المتطلبات الأساسية

المتطلبات

تأكد من استيفاء المتطلبات التالية قبل أن تحاول إجراء هذا التكوين:

- يتم تكوين جدار حماية NetScreen باستخدام عناوين IP على واجهات الثقة/عدم الثقة.
- تم تأسيس الاتصال بالإنترنت.

المكونات المستخدمة

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

- برنامج جدار حماية PIX، الإصدار 6.3(1)

- أحدث مراجعة ل NetScreen

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 (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:

- جدار حماية PIX
- جدار حماية NetScreen

تكوين جدار حماية PIX

جدار حماية PIX
(PIX Version 6.3(1 interface ethernet0 10baset interface ethernet1 100full nameif ethernet0 outside security0 nameif ethernet1 inside security100 enable password 8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU encrypted hostname pixfirewall domain-name cisco.com fixup protocol ftp 21 fixup protocol h323 h225 1720

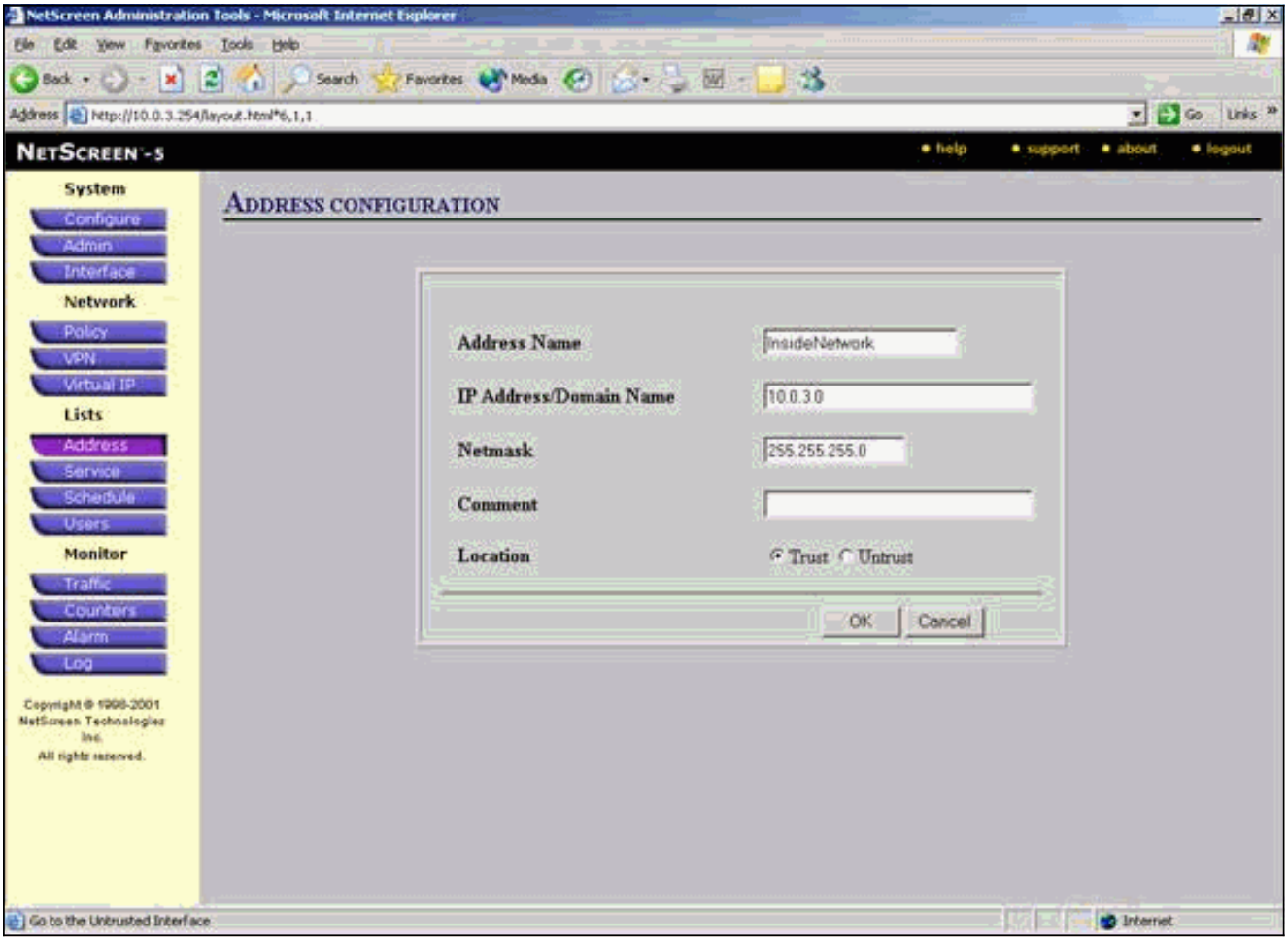
```
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
names
Access control list (ACL) for interesting traffic ---!
to be encrypted and !--- to bypass the Network Address
Translation (NAT) process. access-list nonat permit ip
10.0.25.0 255.255.255.0 10.0.3.0 255.255.255.0
pager lines 24
logging on
logging timestamp
logging buffered debugging
icmp permit any inside
mtu outside 1500
mtu inside 1500
IP addresses on the interfaces. ip address outside ---!
172.18.124.96 255.255.255.0
ip address inside 10.0.25.254 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
pdm logging informational 100
pdm history enable
arp timeout 14400
global (outside) 1 interface
Bypass of NAT for IPsec interesting inside network ---!
traffic. nat (inside) 0 access-list nonat
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
Default gateway to the Internet. route outside ---!
0.0.0.0 0.0.0.0 172.18.124.1 1
timeout xlate 0:05:00
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
http 10.0.0.0 255.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
This command avoids applied ACLs or conduits on ---!
encrypted packets. sysopt connection permit-ipsec
Configuration of IPsec Phase 2. crypto ipsec ---!
transform-set mytrans esp-3des esp-sha-hmac
crypto map mymap 10 ipsec-isakmp
crypto map mymap 10 match address nonat
crypto map mymap 10 set pfs group2
crypto map mymap 10 set peer 172.18.173.85
crypto map mymap 10 set transform-set mytrans
crypto map mymap interface outside
Configuration of IPsec Phase 1. isakmp enable ---!
outside
Internet Key Exchange (IKE) pre-shared key !--- ---!
```

```
that the peers use to authenticate. isakmp key testme
address 172.18.173.85 netmask 255.255.255.255
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash sha
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
dhcpd lease 3600
dhcpd ping_timeout 750
terminal width 80
```

تكوين جدار حماية NetScreen

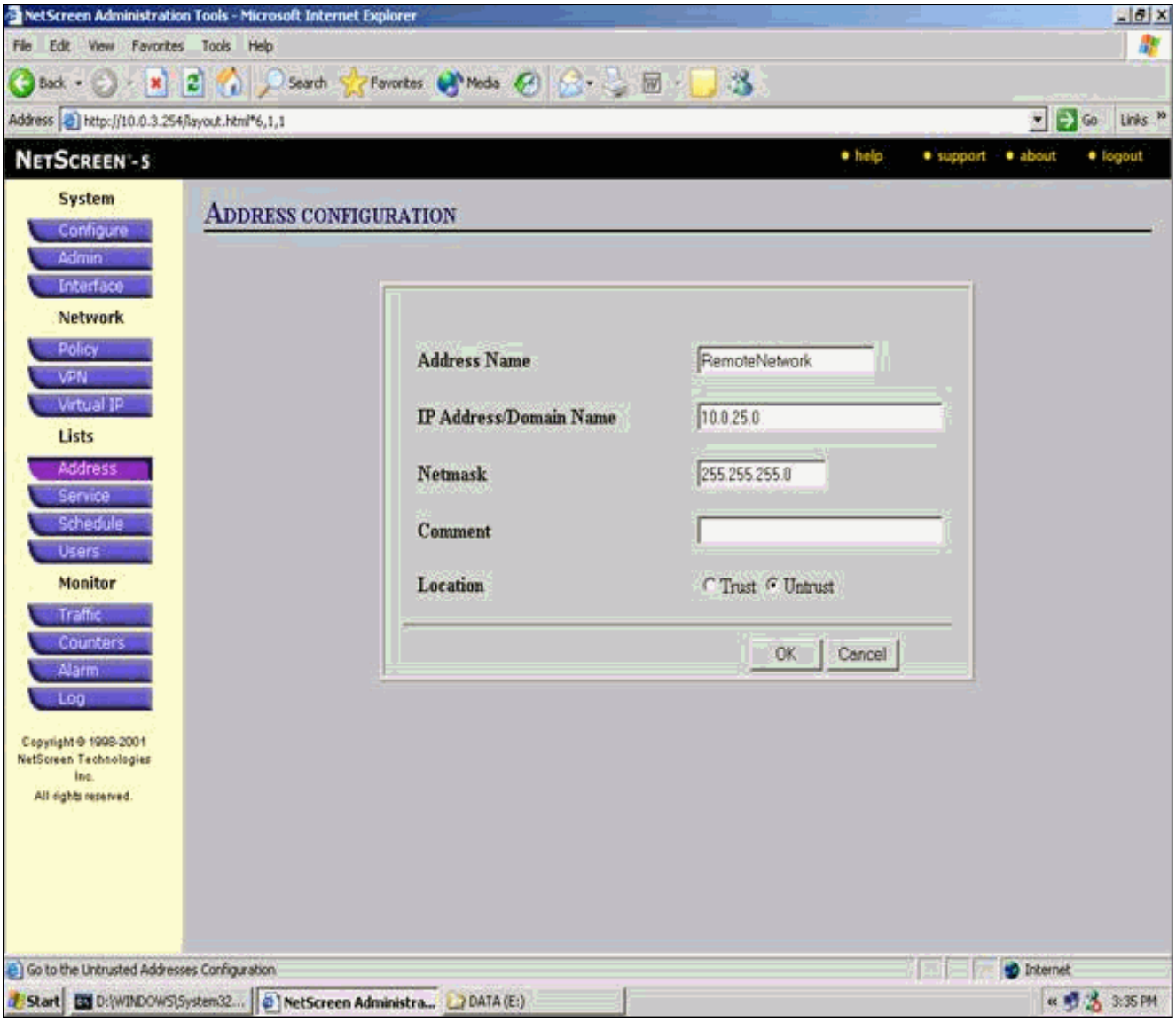
أكمل هذه الخطوات لتكوين جدار حماية NetScreen.

1. حدد **قوائم > عنوان**، انتقل إلى علامة التبويب "موثوق به"، وانقر فوق **عنوان جديد**.
2. أضفت الشبكة الداخلية NetScreen أن يكون شفرت على النفق وطقطقة ok.**ملاحظة:** تأكد من تحديد خيار الثقة.يستخدم هذا المثال الشبكة 10.0.3.0 بقناع 255.255.255.0.

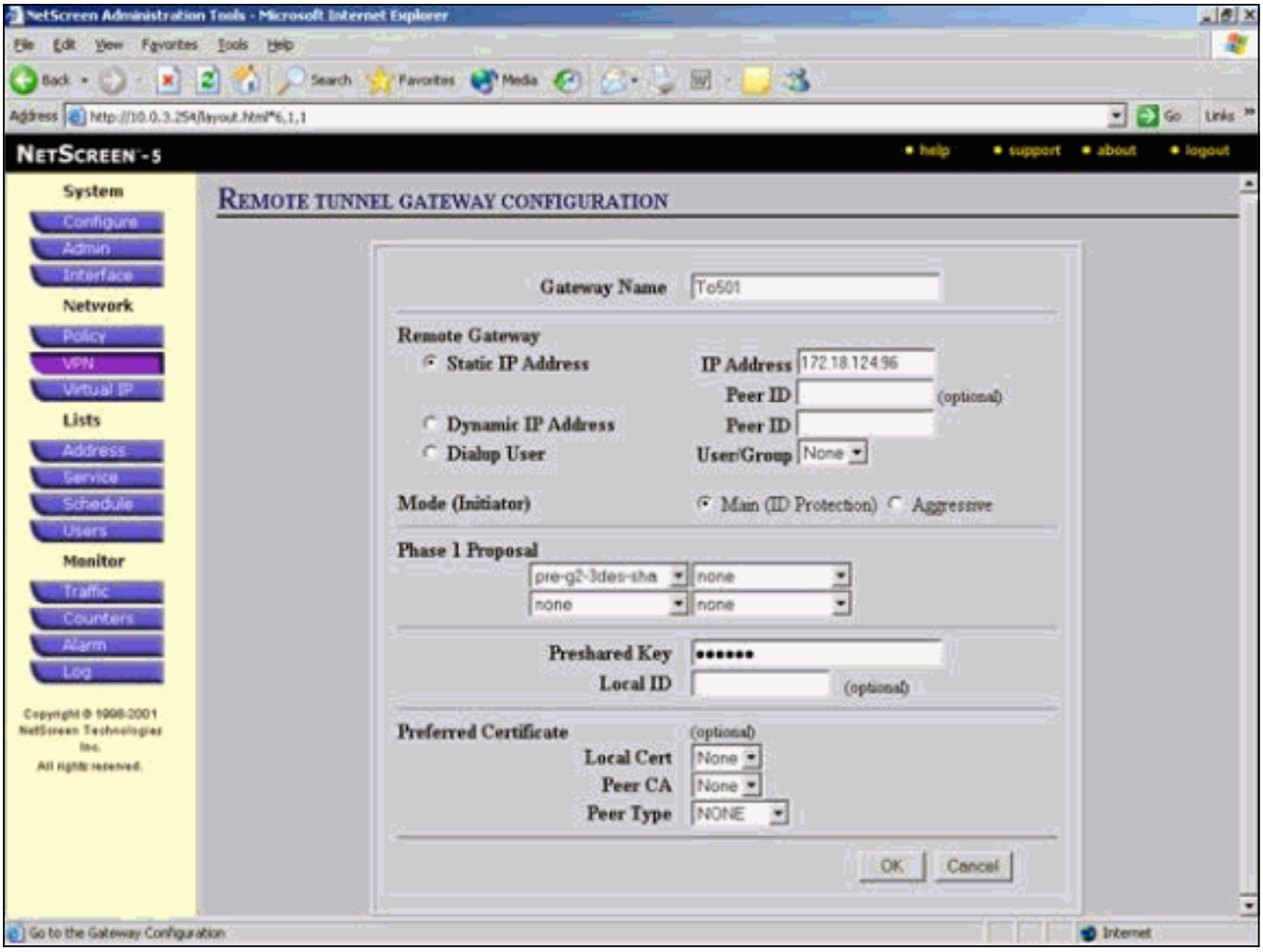


3. حدد **قوائم > عنوان**، انتقل إلى علامة التبويب غير الموثوق بها، وانقر فوق **عنوان جديد**.
4. أضف الشبكة البعيدة التي يستخدمها جدار حماية NetScreen عندما يقوم بتشفير الحزم وانقر فوق **موافق.ملاحظة:** لا تستخدم مجموعات العناوين عند تكوين شبكة VPN إلى بوابة غير NetScreen. يفشل تشغيل VPN البيني إذا كنت تستخدم مجموعات العناوين. لا تعرف بوابة أمان غير NetScreen كيفية ترجمة معرف الوكيل الذي تم إنشاؤه بواسطة NetScreen عند إستخدام مجموعة العناوين.هناك عدة حلول بديلة

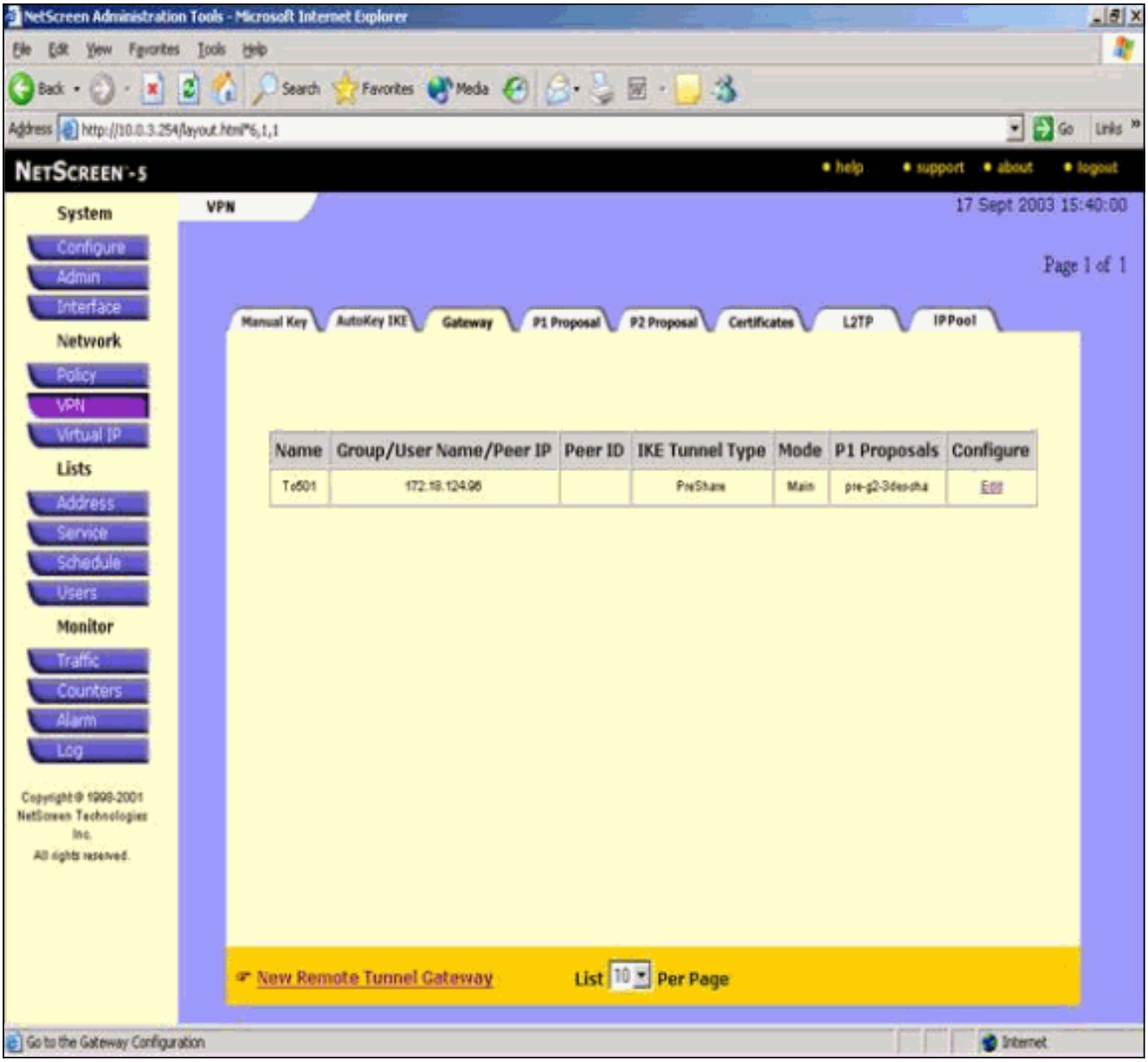
لهذا:افصل مجموعات العناوين إلى إدخالات دفتر عناوين منفردة. حدد السياسات الفردية على أساس إدخال دفتر العناوين.قم بتكوين معرف الوكيل ليكون 0/0.0.0.0 على البوابة غير NetScreen (جهاز جدار الحماية) إذا أمكن.يستخدم هذا المثال الشبكة 10.0.25.0 بقناع
.255.255.255.0



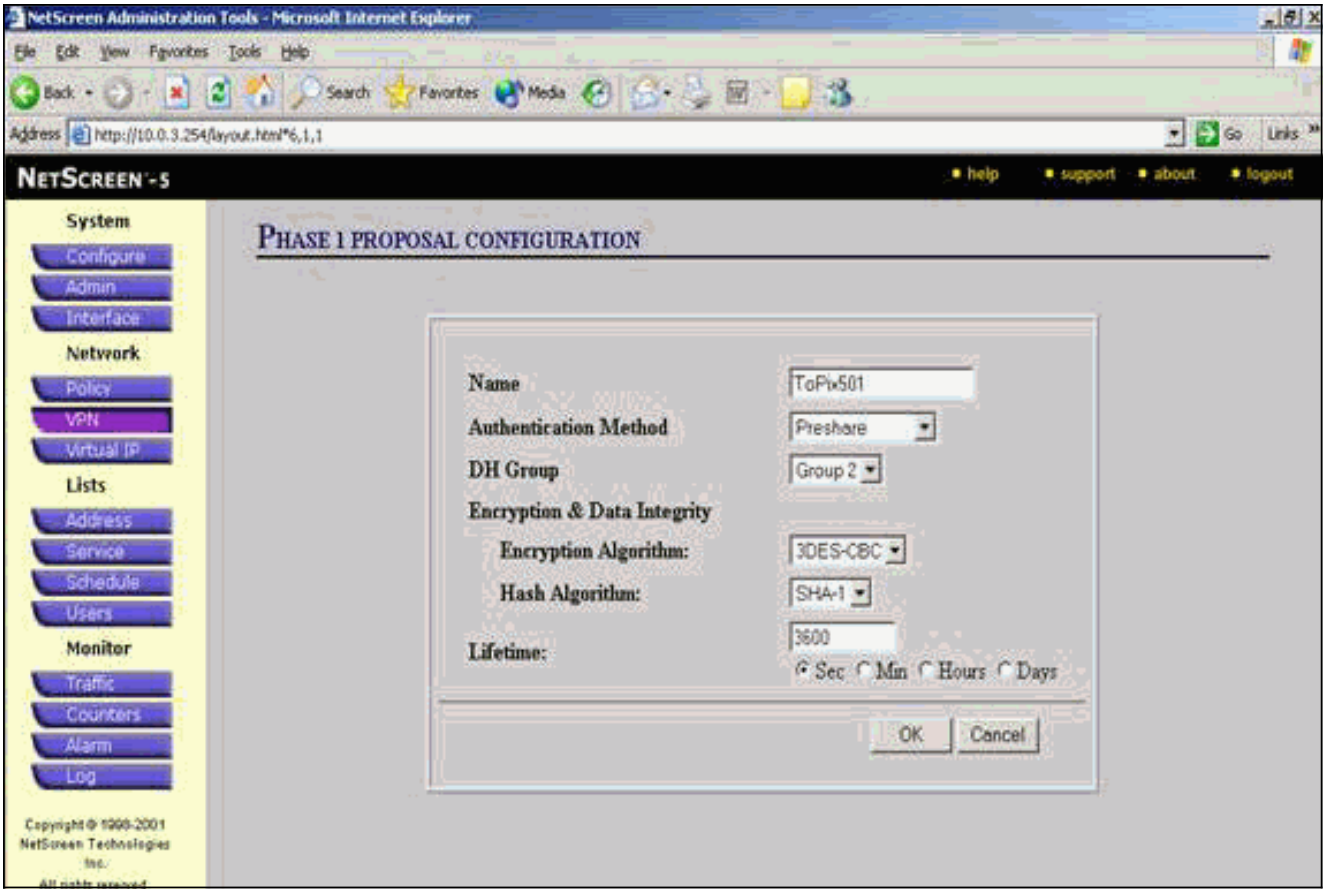
5. حدد **الشبكة > VPN**، انتقل إلى علامة التبويب "العبارة"، وانقر فوق **عبارة النفق البعيد الجديدة** لتكوين عبارة VPN (نهج IPsec للمرحلة 1 والمرحلة 2).
6. أستخدم عنوان IP الخاص بواجهة PIX الخارجية لإنهاء النفق، وتكوين خيارات IKE للمرحلة 1 للربط. طقطقت **ok** عندما أنت إنتهيت.يستخدم هذا المثال هذه الحقول والقيم.**اسم البوابة:** إلى 501**عنوان IP الثابت:**
172.18.124.96**الوضع:** رئيسي (حماية المعرف)**المفتاح المشترك مسبقا:** "testme"**مقترح المرحلة الأولى:** ما قبل الجيل الثاني--3des
sha



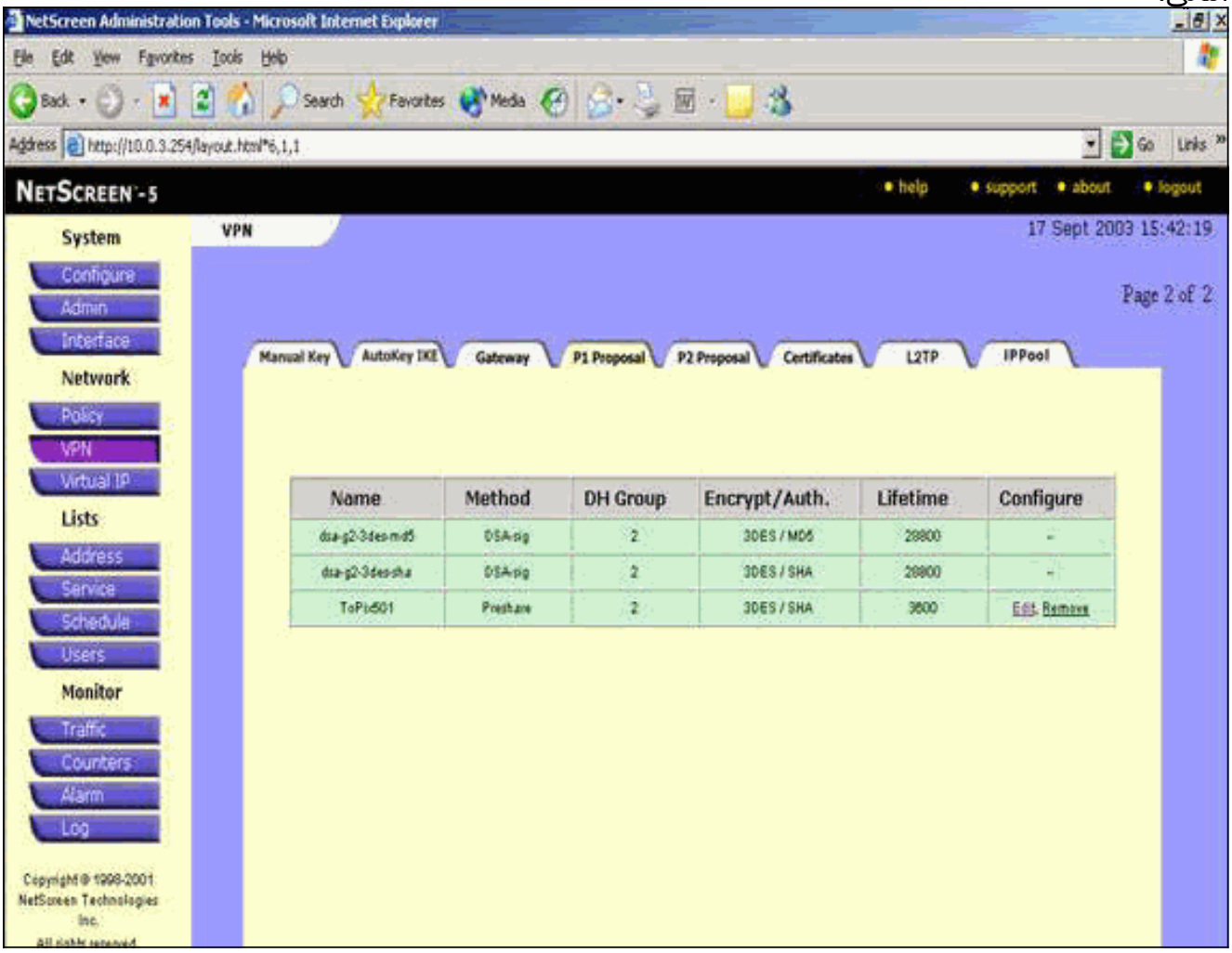
عند إنشاء بوابة النفق البعيد بنجاح، تظهر شاشة مماثلة لهذا.



7. انتقل إلى علامة التبويب "اقتراح P1" وانقر فوق **مقترح المرحلة الجديدة 1** لتكوين المقترح 1.
8. أدخل معلومات التكوين لمقترح المرحلة الأولى وانقر فوق **موافق**.يستخدم هذا المثال هذه الحقول والقيم لتبادل المرحلة الأولى.**الاسم:** ToPIX501**المصادقة:** ما **قبل** الآن**مجموعة DH:** المجموعة 2**التشفير:** 3DES-CBC**التجزئة:** SHA-1**العمر الافتراضي:** 3600 ثانية.

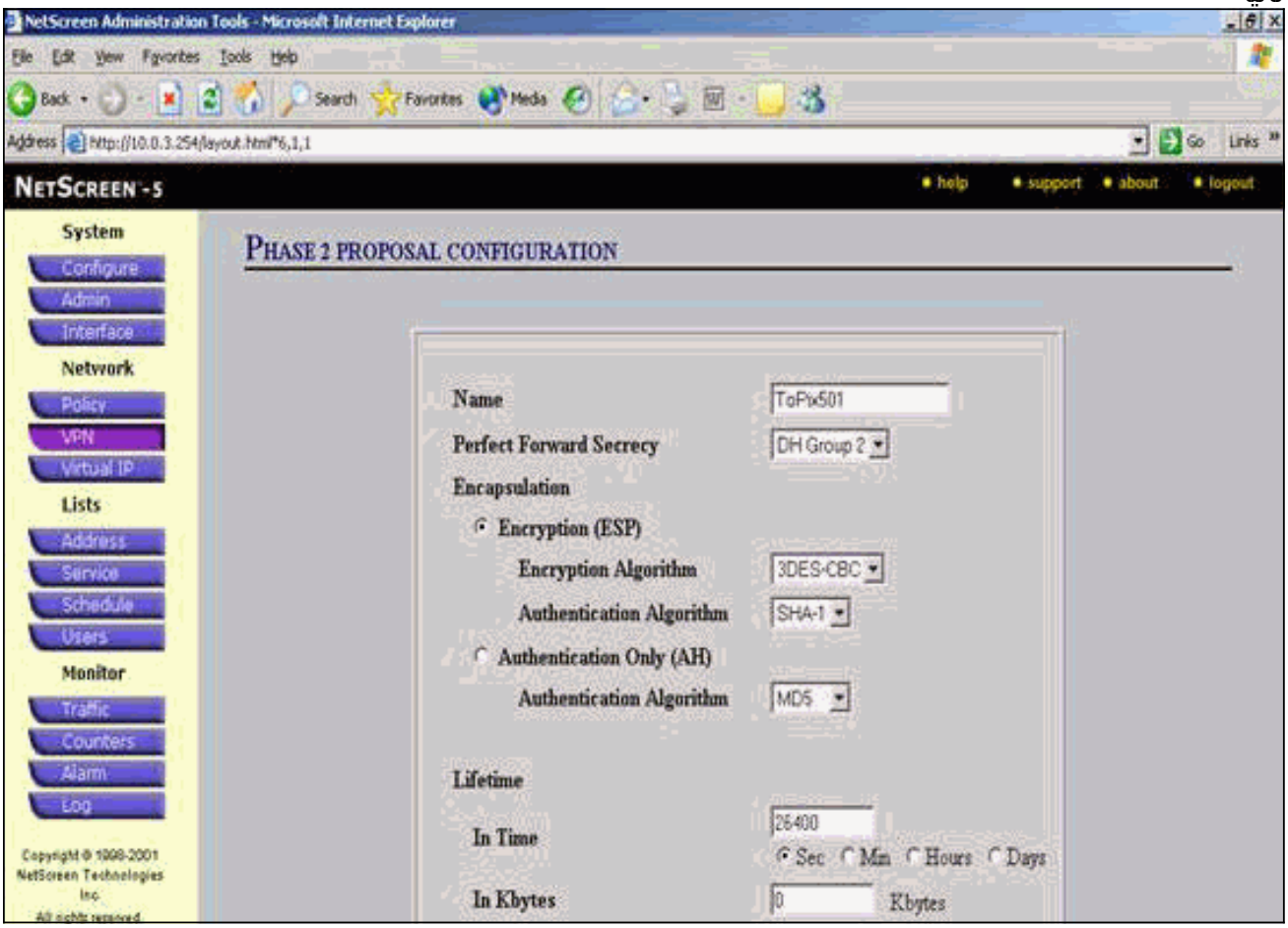


عند إضافة المرحلة 1 بنجاح إلى تكوين NetScreen، تظهر شاشة مماثلة للمثال التالي.

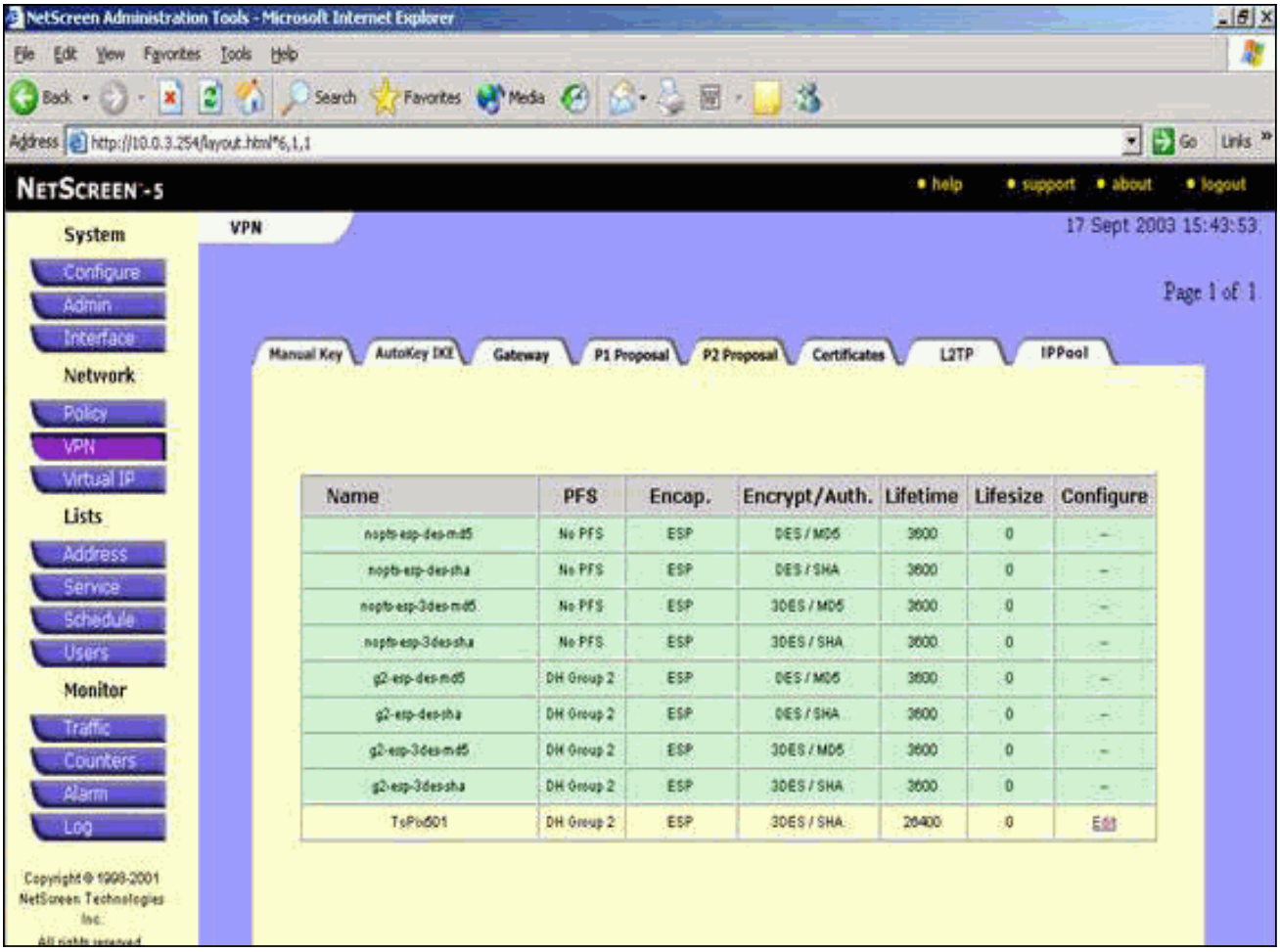


9. انتقل إلى علامة التبويب "مقترح P2" وانقر فوق **مقترح المرحلة الثانية الجديد** لتكوين المرحلة الثانية.

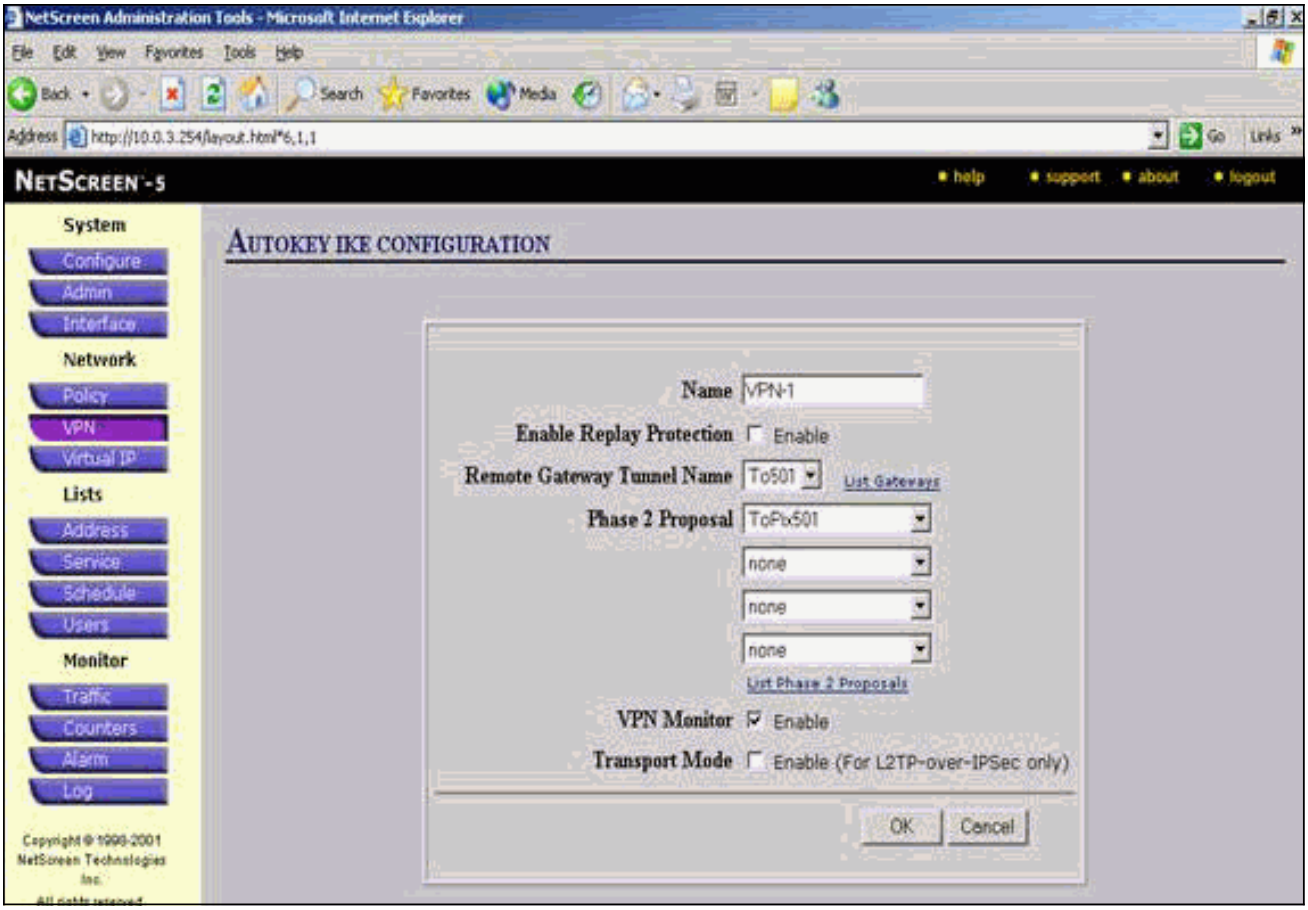
10. أدخل معلومات التكوين لمقترح المرحلة 2 وانقر فوق **موافق**.يستخدم هذا المثال هذه الحقول والقيم لتبادل المرحلة 2.**الاسم:** ToPIX501**سرية إعادة التوجيه المثالية:** 1024) 2-DH بت)**خوارزمية التشفير:** 3DES-CBC**خوارزمية المصادقة:** SHA-1**مدى الحياة:** 26400 ثانية



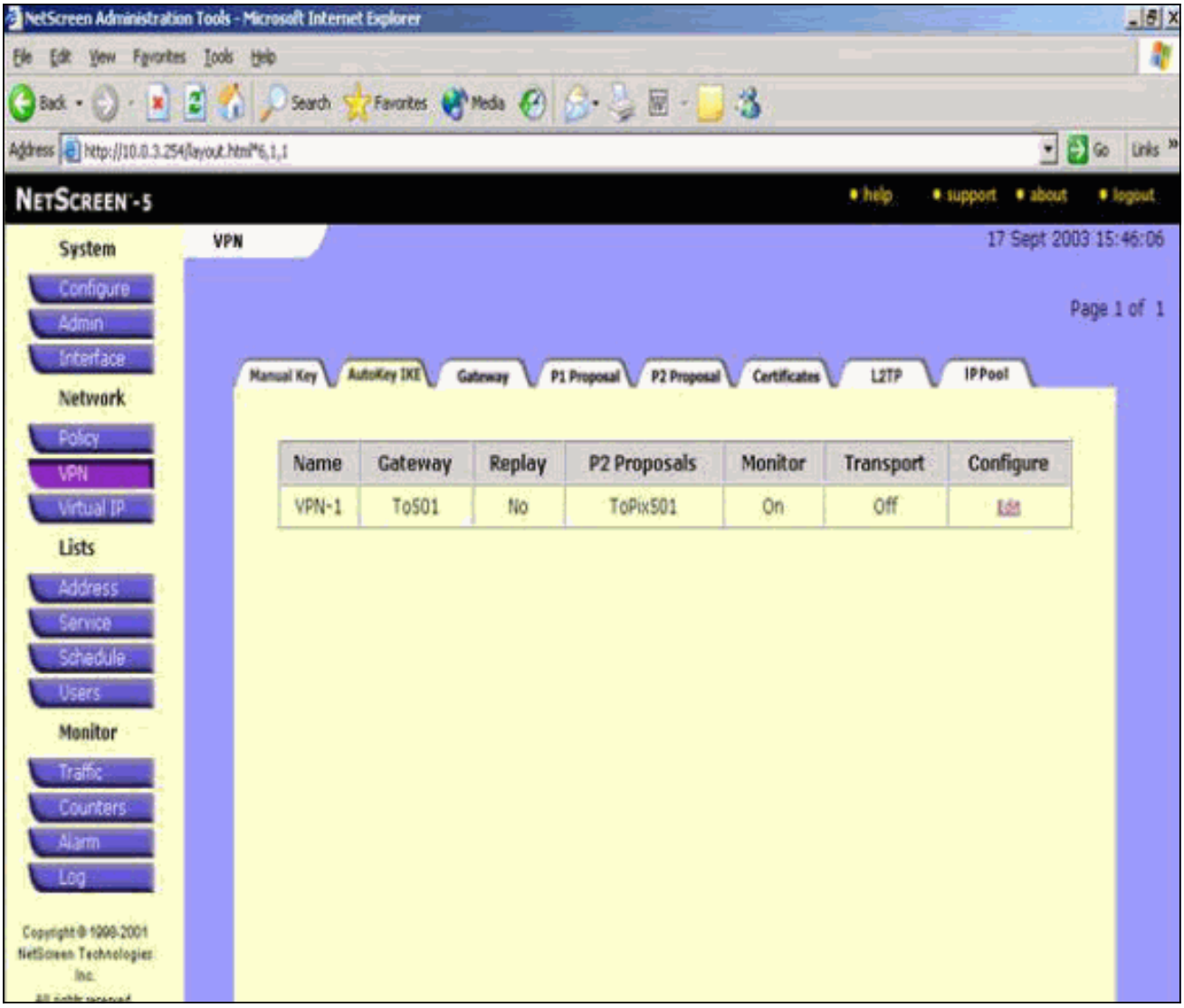
عند إضافة المرحلة 2 بنجاح إلى تكوين NetScreen، تظهر شاشة مماثلة للمثال التالي.



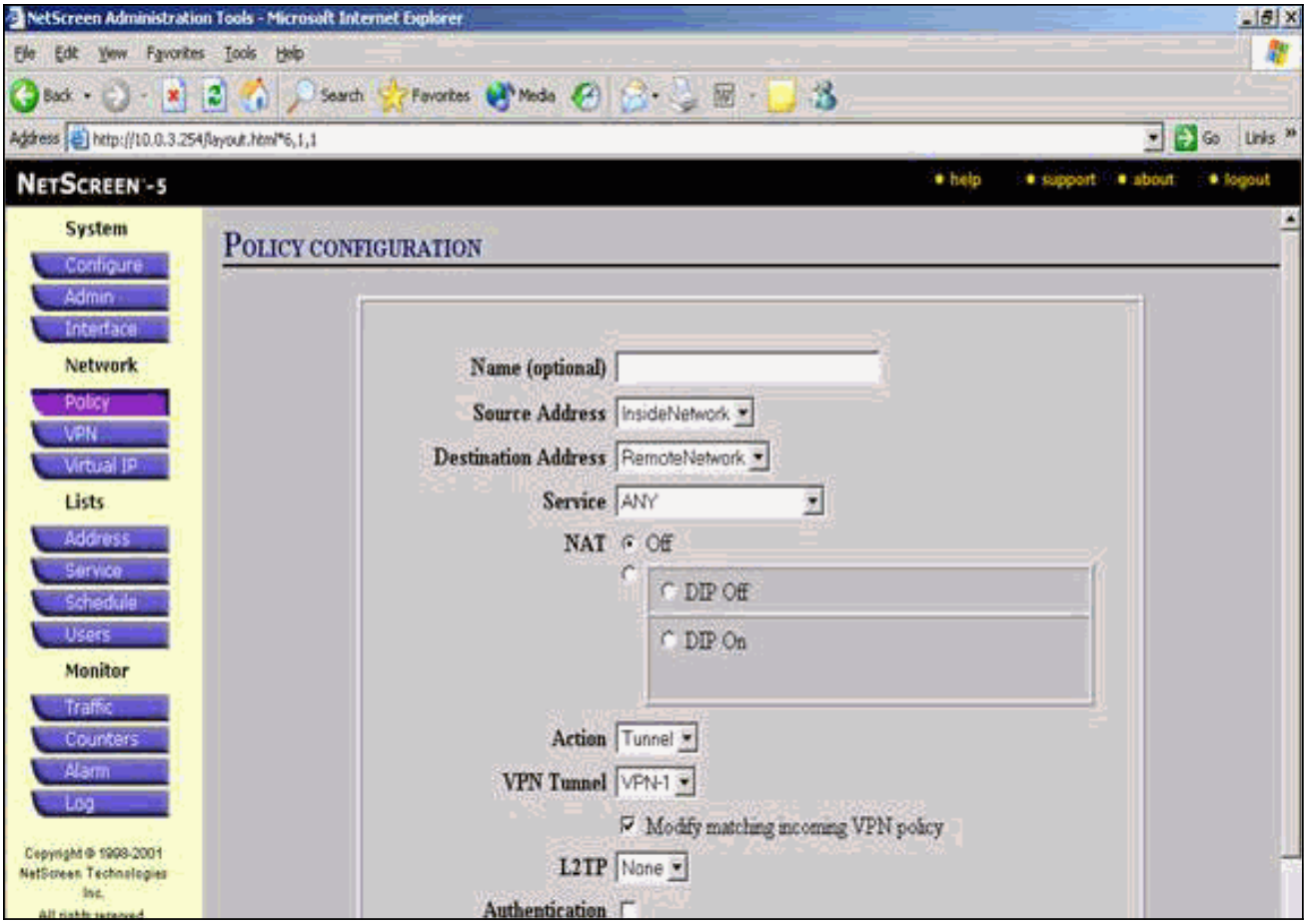
11. حدد علامة التبويب **AutoKey IKE**، ثم انقر فوق **إدخال AutoKey IKE الجديد** لإنشاء IKE AutoKeys وتكوينه.
12. أدخل معلومات التكوين ل AutoKey IKE، ثم انقر فوق **موافق**.يستخدم هذا المثال هذه الحقول والقيم ل AutoKey IKE.**الاسم:** VPN-1**اسم نفق العبارة البعيدة:**to501(تم إنشاء هذا مسبقا في علامة التبويب "البوابة".)**مقترح المرحلة الثانية:** ToPIX501(تم إنشاء ذلك مسبقا في علامة التبويب "اقتراح P2".)**شاشة VPN:** تمكين(هذا يمكن جهاز NetScreen من ضبط ملائمات بروتوكول إدارة الشبكة البسيط [SNMP] لمراقبة حالة شاشة VPN.)



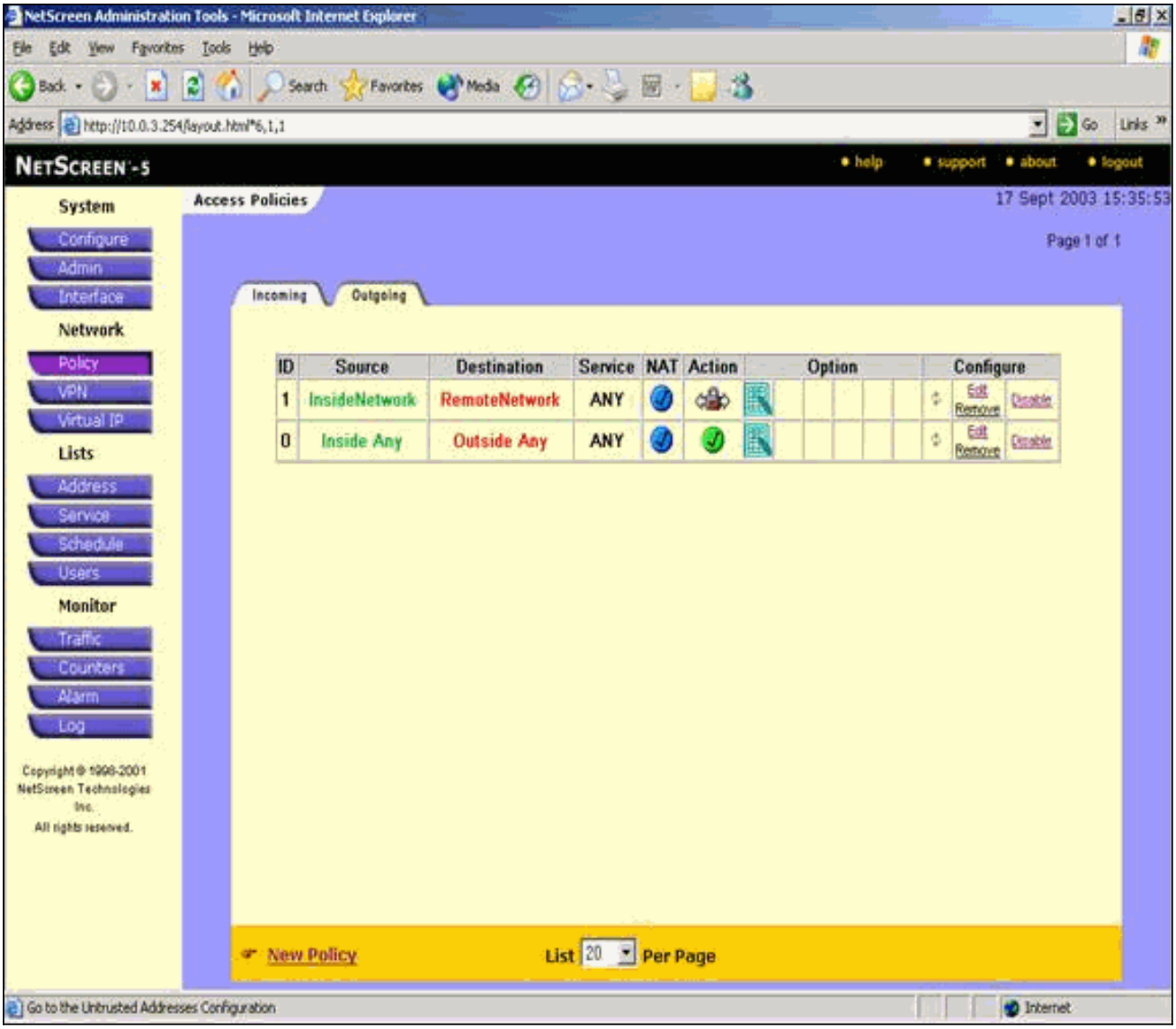
عند تكوين قاعدة VPN-1 بنجاح، تظهر شاشة مماثلة للمثال التالي.



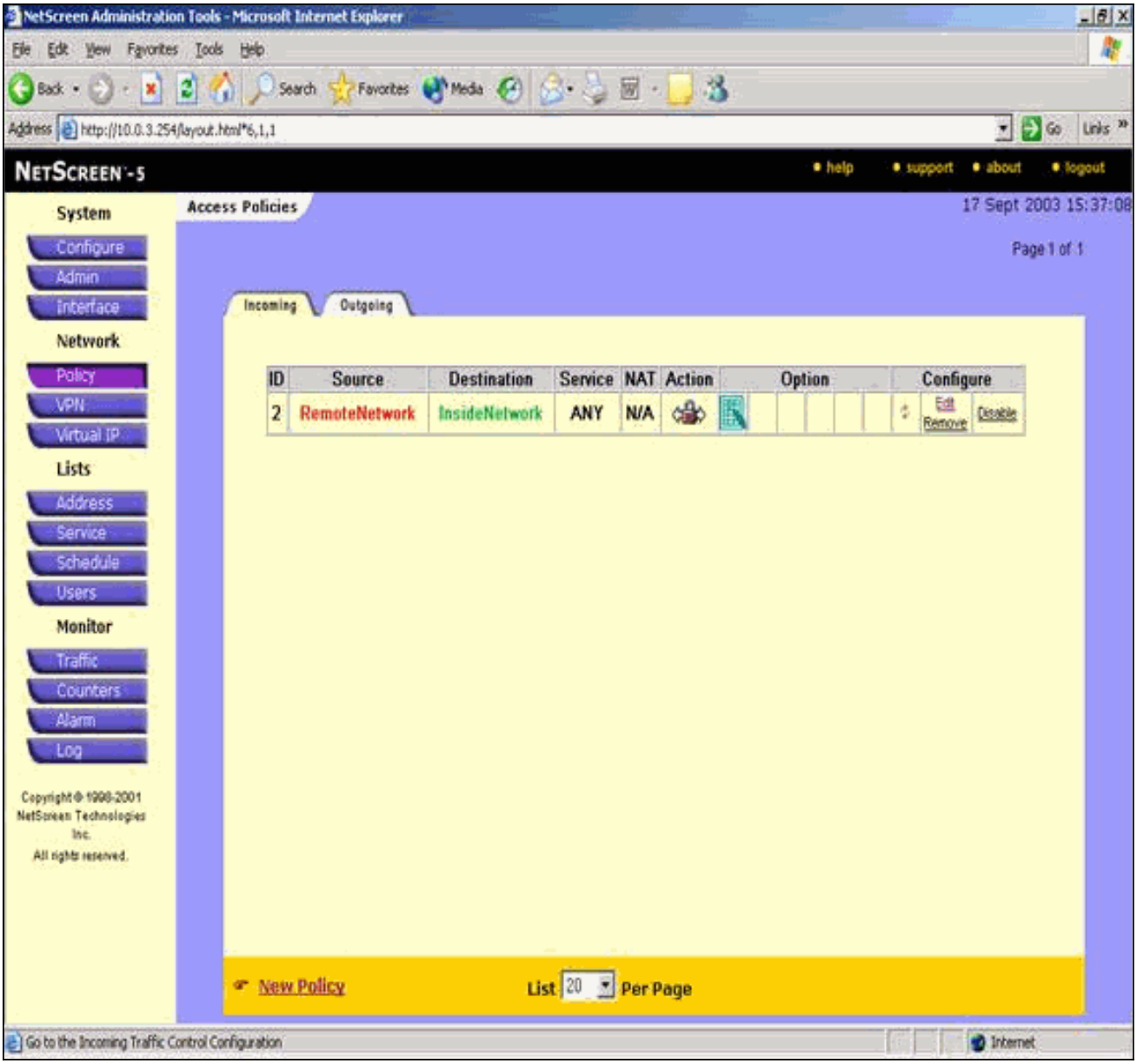
13. حدد **شبكة > سياسة**، انتقل إلى علامة التبويب "الصادر"، وانقر فوق **نهج جديد** لتكوين القواعد التي تسمح بتشفير حركة مرور IPsec.
14. أدخل معلومات التكوين للنهج وانقر فوق **موافق**.يستخدم هذا المثال هذه الحقول والقيم للنهج. حقل "الاسم" إختياري ولا يتم إستخدامه في هذا المثال.**عنوان المصدر:** داخل الشبكة(تم تحديد هذا مسبقا في علامة التبويب "موثوق".)**غاية عنوان:** شبكة بعيد(تم تحديد هذا مسبقا ضمن علامة التبويب غير الموثوق بها.)**الخدمة:** أي**عملية:** نفق**نفق VPN:** VPN-1(كان هذا قد تم تعريفه من قبل على أنه نفق VPN في علامة تبويب AutoKey IKE.)**تعديل نهج VPN الوارد المطابق:** محدد(يقوم هذا الخيار تلقائيا بإنشاء قاعدة واردة تطابق حركة مرور VPN الخارجية للشبكة.)



15. عند إضافة النهج، تأكد من أن قاعدة VPN الصادرة هي الأولى في قائمة السياسات. (القاعدة التي يتم إنشاؤها تلقائيا لحركة المرور الواردة موجودة في علامة التبويب الواردة.)أتمت هذا steps إن يحتاج أنت أن يغير الترتيب من السياسة:انقر صفحة الصادر.انقر فوق الأسهم الدائرية في عمود التكوين لعرض نافذة نقل النهج الدقيقة.قم بتغيير ترتيب السياسات بحيث تكون سياسة الشبكة الخاصة الظاهرية (VPN) أعلى معرف السياسة 0 (بحيث يكون نهج الشبكة الخاصة الظاهرية (VPN) في أعلى القائمة).



انتقل إلى علامة التبويب الوارد لعرض قاعدة حركة المرور الواردة.



التحقق من الصحة

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

أوامر التحقق

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

- **ping**—تشخيص الاتصال الأساسي بالشبكة.
- **show crypto ipSec**—يعرض اقترانات أمان المرحلة 2.
- **show crypto isakmp sa**—يعرض اقترانات أمان المرحلة 1.

ناتج التحقق

يتم عرض نموذج الإخراج من **أوامر ping** و**show** هنا.

يتم بدء إختبار الاتصال هذا من مضيف خلف جدار حماية NetScreen.

```
C:\>ping 10.0.25.1 -t
.Request timed out
.Request timed out
Reply from 10.0.25.1: bytes=32 time<105ms TTL=128
Reply from 10.0.25.1: bytes=32 time<114ms TTL=128
Reply from 10.0.25.1: bytes=32 time<106ms TTL=128
Reply from 10.0.25.1: bytes=32 time<121ms TTL=128
Reply from 10.0.25.1: bytes=32 time<110ms TTL=128
Reply from 10.0.25.1: bytes=32 time<116ms TTL=128
Reply from 10.0.25.1: bytes=32 time<109ms TTL=128
Reply from 10.0.25.1: bytes=32 time<110ms TTL=128
Reply from 10.0.25.1: bytes=32 time<118ms TTL=128
```

يتم عرض الإخراج من الأمر **show crypto ipSec sa** هنا.

```
pixfirewall(config)#show crypto ipsec sa

interface: outside
Crypto map tag: mymap, local addr. 172.18.124.96

:(local  ident (addr/mask/prot/port
(10.0.25.0/255.255.255.0/0/0)
:(remote ident (addr/mask/prot/port
(10.0.3.0/255.255.255.0/0/0)
current_peer: 172.18.173.85:500
{,PERMIT, flags={origin_is_acl
pkts encaps: 11, #pkts encrypt: 11, #pkts digest 11#
pkts decaps: 11, #pkts decrypt: 13, #pkts verify 13#
pkts compressed: 0, #pkts decompressed: 0#
,pkts not compressed: 0, #pkts compr. failed: 0#
pkts decompress failed: 0, #send errors 0, #recv errors 1#

,local crypto endpt.: 172.18.124.96
remote crypto endpt.: 172.18.173.85
path mtu 1500, ipsec overhead 56, media mtu 1500
current outbound spi: f0f376eb

:inbound esp sas
(spi: 0x1225ce5c(304467548
, transform: esp-3des esp-sha-hmac
{ ,in use settings ={Tunnel
slot: 0, conn id: 3, crypto map: mymap
:(sa timing: remaining key lifetime (k/sec
(4607974/24637)
IV size: 8 bytes
replay detection support: Y

:inbound ah sas

:inbound pcp sas

:outbound esp sas
(spi: 0xf0f376eb(4042487531
, transform: esp-3des esp-sha-hmac
{ ,in use settings ={Tunnel
slot: 0, conn id: 4, crypto map: mymap
:(sa timing: remaining key lifetime (k/sec
(4607999/24628)
IV size: 8 bytes
replay detection support: Y

:outbound ah sas
```

```
:outbound pcp sas
```

يتم عرض الإخراج من الأمر **show crypto isakmp sa** هنا.

```
pixfirewall(config)#show crypto isakmp sa
                                    Total     : 1
                                    Embryonic : 0
dst             src          state   pending  created
   QM_IDLE      0        1  172.18.173.85  172.18.124.96
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

أوامر استكشاف الأخطاء وإصلاحها

ملاحظة: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل إستخدام أوامر **debug**.

- **debug crypto engine**—يعرض رسائل حول محركات التشفير.
- **debug crypto ipSec**—يعرض معلومات حول أحداث IPsec.
- **debug crypto isakmp**—يعرض الرسائل المتعلقة بأحداث IKE.

إخراج تصحيح الأخطاء للعينة

يتم عرض إخراج **تصحيح الأخطاء** للعينة من جدار حماية PIX هنا.

```
debug crypto engine
 debug crypto ipsec
debug crypto isakmp

,crypto_isakmp_process_block:src:172.18.173.85
          dest:172.18.124.96 spt:500 dpt:500
                                OAK_MM exchange
ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy
                      ISAKMP:      encryption 3DES-CBC
                                ISAKMP:      hash SHA
                             ISAKMP:      default group 2
                              ISAKMP:      auth pre-share
                          ISAKMP:      life type in seconds
                ISAKMP:      life duration (basic) of 28800
        ISAKMP (0): atts are acceptable. Next payload is 0
                   ISAKMP (0): processing vendor id payload

                   ISAKMP (0): processing vendor id payload

ISAKMP (0): SA is doing pre-shared key authentication
                            using id type ID_IPV4_ADDR
                          return status is IKMP_NO_ERROR
,crypto_isakmp_process_block:src:172.18.173.85
          dest:172.18.124.96 spt:500 dpt:500
                                OAK_MM exchange
ISAKMP (0): processing KE payload. message ID = 0

ISAKMP (0): processing NONCE payload. message ID = 0
```

```
                                    return status is IKMP_NO_ERROR
                        ,crypto_isakmp_process_block:src:172.18.173.85
                                dest:172.18.124.96 spt:500 dpt:500
                                                    OAK_MM exchange
                  ISAKMP (0): processing ID payload. message ID = 0
                ISAKMP (0): processing HASH payload. message ID = 0
                                ISAKMP (0): SA has been authenticated

                                                  ISAKMP (0): ID payload
                                                next-payload : 8
                                                type         : 1
                                               protocol     : 17
                                              port         : 500
                                                length       : 8
                                     ISAKMP (0): Total payload length: 12
                                            return status is IKMP_NO_ERROR
                               ISAKMP (0): sending INITIAL_CONTACT notify
                          ISAKMP (0): sending NOTIFY message 24578 protocol 1
                    VPN Peer: ISAKMP: Added new peer: ip:172.18.173.85/500
                                                    Total VPN Peers:1
                       VPN Peer: ISAKMP: Peer ip:172.18.173.85/500 Ref cnt
                                                     incremented to:1
                                                    Total VPN Peers:1
                        ,crypto_isakmp_process_block:src:172.18.173.85
                                dest:172.18.124.96 spt:500 dpt:500
      ,ISAKMP (0): processing DELETE payload. message ID = 534186807
                                    spi size = 4IPSEC(key_engin
                                          ...e): got a queue event
       IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
                                     :(IPSEC(key_engine_delete_sas
                           delete all SAs shared with 172.18.173.85

                                    return status is IKMP_NO_ERR_NO_TRANS
                        ,crypto_isakmp_process_block:src:172.18.173.85
                                dest:172.18.124.96 spt:500 dpt:500
                                                    OAK_QM exchange
                                oakley_process_quick_mode: OAK_QM_IDLE
          ISAKMP (0): processing SA payload. message ID = 4150037097

                                     ISAKMP : Checking IPSec proposal 1

                                          ISAKMP: transform 1, ESP_3DES
                                    :ISAKMP:   attributes in transform
                                  ISAKMP:      SA life type in seconds
            ISAKMP:      SA life duration (VPI) of 0x0 0x0 0x67 0x20
                                       ISAKMP:      encaps is 1
                             ISAKMP:      authenticator is HMAC-SHA
                                         ISAKMP:      group is 2
                                    .ISAKMP (0): atts are acceptable
                  ,IPSEC(validate_proposal_request): proposal part #1
          ,key eng. msg.) dest= 172.18.124.96, src= 172.18.173.85)
               ,(dest_proxy= 10.0.25.0/255.255.255.0/0/0 (type=4
                 ,(src_proxy= 10.0.3.0/255.255.255.0/0/0 (type=4
               , protocol= ESP, transform= esp-3des esp-sha-hmac
                                       ,lifedur= 0s and 0kb
                spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x24

       ISAKMP (0): processing NONCE payload. message ID = 4150037097

          ISAKMP (0): processing KE payload. message ID = 4150037097

          ISAKMP (0): processing ID payload. message ID = 4150037097
          ISAKMP (0): ID_IPV4_ADDR_SUBNET src 10.0.3.0/255.255.255.0
```

```
                                                    prot 0 port 0
                    ISAKMP (0): processing ID payload. message ID = 4150037097
                  ISAKMP (0): ID_IPV4_ADDR_SUBNET dst 10.0.25.0/255.255.255.0
                                        (prot 0 port 0IPSEC(key_engine
                                                ...got a queue event :
              IPSEC(spi_response): getting spi 0x1225ce5c(304467548) for SA
                 from   172.18.173.85 to   172.18.124.96 for prot 3

                                                return status is IKMP_NO_ERROR
                                    ,crypto_isakmp_process_block:src:172.18.173.85
                                             dest:172.18.124.96 spt:500 dpt:500
                                                          OAK_QM exchange
                                                :oakley_process_quick_mode
                                    OAK_QM_AUTH_AWAITmap_alloc_entry: allocating entry 3
                                                map_alloc_entry: allocating entry 4

                                                ISAKMP (0): Creating IPSec SAs
                                inbound SA from 172.18.173.85 to 172.18.124.96
                                                (proxy 10.0.3.0 to 10.0.25.0)
                                  has spi 304467548 and conn_id 3 and flags 25
                                                lifetime of 26400 seconds
                                outbound SA from 172.18.124.96 to 172.18.173.85
                                                (proxy 10.0.25.0 to 10.0.3.0)
                                 has spi 4042487531 and conn_id 4 and flags 25
            ...lifetime of 26400 secondsIPSEC(key_engine): got a queue event
                                                        , :(IPSEC(initialize_sas
                          ,key eng. msg.) dest= 172.18.124.96, src= 172.18.173.85)
                                ,(dest_proxy= 10.0.25.0/255.255.255.0/0/0 (type=4
                                  ,(src_proxy= 10.0.3.0/255.255.255.0/0/0 (type=4
                                , protocol= ESP, transform= esp-3des esp-sha-hmac
                                                    ,lifedur= 26400s and 0kb
                                            ,spi= 0x1225ce5c(304467548), conn_id= 3
                                                keysize= 0, flags= 0x25
                                                        , :(IPSEC(initialize_sas
                          ,key eng. msg.) src= 172.18.124.96, dest= 172.18.173.85)
                                 ,(src_proxy= 10.0.25.0/255.255.255.0/0/0 (type=4
                                 ,(dest_proxy= 10.0.3.0/255.255.255.0/0/0 (type=4
                                , protocol= ESP, transform= esp-3des esp-sha-hmac
                                                    ,lifedur= 26400s and 0kb
               spi= 0xf0f376eb(4042487531), conn_id= 4, keysize= 0, flags= 0x25

                                VPN Peer: IPSEC: Peer ip:172.18.173.85/500 Ref cnt
                                            incremented to:2 Total VPN Peers:1
                                VPN Peer: IPSEC: Peer ip:172.18.173.85/500 Ref cnt
                                            incremented to:3 Total VPN Peers:1
                                                return status is IKMP_NO_ERROR
```

معلومات ذات صلة

- مفاوضة IPSec/بروتوكولات IKE
- برنامج جدار حماية Cisco PIX
- مراجع أوامر جدار حماية PIX الآمن من Cisco
- الإعلامات الميدانية لمنتج الأمان (بما في ذلك PIX)
- 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).