# رادج نيب LAN ىلIPSec LAN قفن نيوكت قيامح رادجو Cisco PIX قيامح NetScreen

## المحتويات

<u>المقدمة</u> <u>المتطلبات الأساسية</u> <u>المكونات المستخدمة</u> <u>الاصطلاحات</u> <u>التكوين</u> <u>الرسم التخطيطي للشبكة</u> <u>التحقق من الصحة</u> <u>أوامر التحقق</u> <u>أوامر التحقق</u> <u>أوامر استكشاف الأخطاء وإصلاحها</u> <u>إخراج تصحيح الأخطاء للعينة</u> معلومات ذات صلة

## <u>المقدمة</u>

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.

## <u>المتطلبات الأساسية</u>

#### <u>المتطلبات</u>

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.

#### <u>المكونات المستخدمة</u>

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 المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

#### <u>الاصطلاحات</u>

راجع <u>اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.</u>

## <u>التكوين</u>

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

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

#### <u>الرسم التخطيطي للشبكة</u>

يستخدم هذا المستند إعداد الشبكة التالي:



#### <u>التكوينات</u>

يستخدم هذا المستند التكوينات التالية:

- <u>جدار حماية PIX</u>
- <u>جدار حماية NetScreen</u>

#### <u>تكوين جدار حماية PIX</u>

|          | جدار حمایة PIX                     |
|----------|------------------------------------|
|          |                                    |
|          | (PIX Version 6.3(1                 |
|          | interface ethernet0 10baset        |
|          | interface ethernet1 100full        |
|          | nameif ethernet0 outside security0 |
| n        | ameif ethernet1 inside security100 |
| enable p | assword 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
```

<u>تکوین جدار حمایة NetScreen</u>

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 o**k.ملاحظة:** تأكد من تحديد خيار الثقة.يستخدم هذا المثال الشبكة 10.0.3.0 بقناع

|   | Search Kraverces                       |                   |                 |
|---|--|-------------------|-----------------|
| ass ) http://10.0.3.254/layout.html*6,1,  | 1.                                     |                   | <u>.</u>        |
| ETSCREEN'-5                               |  | • help • suppor   | t • about • log |
| System ADDRE                              | SS CONFIGURATION                       |                   |                 |
| Admin                                     |  |                   |                 |
| Interface                                 | 1                                      | 1                 |                 |
| Network                                   |  |                   |                 |
| Policy                                    | Address Name                           | [insideNetwork    |                 |
| VPN<br>Virtual IP                         | 10000000000000000000000000000000000000 |                   |                 |
| Lists                                     | IP Address/Domain Name                 | 10.0.3.0          |                 |
| Address                                   | Netmask                                | 255 255 255 0     |                 |
| Service                                   | 2012/00/2009<br>(2012/2012/2019)       |                   |                 |
| Schedule                                  | Comment                                |                   |                 |
| Monitor                                   | Location                               | G Trust C Untrust |                 |
| Traffic                                   | 2101/1/24/96                           |                   |                 |
| Counters                                  |  | OK Cancel         |                 |
| Alarm                                     | P                                      |                   |                 |
|   |  |                   |                 |
| pyrigM © 1996-2001<br>Screen Technologiez |  |                   |                 |
| All rights reserved.                      |  |                   |                 |
|   |  |                   |                 |
|   |  |                   |                 |

- 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 0/0.0.00 على البوابة غير NetScreen (جهاز جدار الحماية) إذا أمكن.يستخدم هذا المثال الشبكة 10.0.25.0 بقناع

.255.255.255.0

|   |                                    | .200.200.20  | ) <u>)</u> .c      |
|---|------------------------------------|--|--------------------|
| NetScreen Administration Tools - Micro                          | soft Internet Explorer             |  | 18 ×               |
| File Edit View Favorites Tools Help                             |                                    | - 1000 200 A   | 4                  |
| 🔾 Back • 🕗 · 🖹 🚨 🏠 🌽  | Search 🎇 Favorites 💕 Media 🚱 🔂 🤤 🐚 | 1 · 🔁 🍊 .  |                    |
| Address Altp://10.0.3.254/kayout.html*6,1,                      | 1                                  | - D 🗠 🛛  | inis <sup>10</sup> |
| NETSCREEN'-5  |                                    | <ul> <li>help</li> <li>support</li> <li>about</li> <li>logo</li> </ul> | jut.               |
| System  |                                    |  |                    |
| Configure   | SS CONFIGURATION                   |  | _6                 |
| Admin   |                                    |  |                    |
| Interface   | 0                                  |  |                    |
| Network   |                                    |  |                    |
| Policy  | Address Name                       | RemoteNetwork  |                    |
| Vetual IP   |                                    |  |                    |
| Lists   | IP Address/Domain Name             | 10.0.25.0  |                    |
| Address   | Netmask                            | 255 255 255 0  |                    |
| Service   | 2 Metrodeval                       |  |                    |
| Schedule  | Comment                            |  |                    |
| Users   |                                    |  |                    |
| Monitor   | Location                           | C Trust @ Untrust  |                    |
| Counters  | -                                  |  |                    |
| Alarm   |                                    | OK   |                    |
| Log   |                                    |  |                    |
| Cepyright @ 1998-2001   |                                    |  |                    |
| NetScreen Technologies<br>Inc.                                  |                                    |  |                    |
| All rights reserved.  |                                    |  |                    |
|   |                                    |  |                    |
|   |                                    |  |                    |
|   |                                    |  |                    |
|   |                                    |  |                    |
| <ul> <li>Go to the Untrusted Addresses Configuration</li> </ul> |                                    | 🔄 🗍 👘 💓 Internet   | =                  |
| 🐮 Start 🔤 D:{WINDOWS{5ystem32                                   | NetScreen Administra 🔛 DATA (E:)   |  | IS PM              |

- 5. حدد **الشبكة > VPN**، انتقل إلى علامة التبويب "العبارة"، وانقر فوق **عبارة النفق البعيد الجديدة** لتكوين عبارة (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:** قبل الجيل الثاني--3de sha

| NetScreen Administration Tools - Micros         | soft Internet Explorer                                   | @X           |
|---|--|--------------|
| Ele Edit Yew Favorites Jools Help               |  | 2            |
| 🔾 tack + 🔘 - 💌 🖻 🐔 🔎                            | Search 👷 Favorites 😸 Media 🌮 🍰 🐨 - 🤤 📸                   |              |
| Agaress Antp://10.0.3.254/layout.html*6,1,      | 1  | 🔂 Go Links » |
| NETSCREEN'-5                                    | • help · • support • about                               | t • lagout   |
| System Dragon                                   | E TINNET CATERIAN CONFICUERATION                         | <u>.</u>     |
| Configure                                       | E TUNNEL GATEWAT CONFIGURATION                           | [            |
| Admin   |  |              |
| Interface                                       | Gateway Name To501                                       |              |
| Network   | Remote Gateway   |              |
| VPN   | © Static IP Address IP Address 172.18.124.96             |              |
| Virtual IP                                      | Peer ID (optional)                                       |              |
| Lists   | C Dynamic IP Address Peer ID                             |              |
| Address   | C Dialup User User/Group None 🛨                          |              |
| Service<br>Criteriale                           | Made (Initiator) (F. Man (II) Protection) (F. Annecessor |              |
| Users   | Frank (mentality) Frank (mentality) Frank                |              |
| Monitor   | Phase 1 Proposal   |              |
| Traffic   | none × none •  |              |
| Counters  |  |              |
| Log   | Preshared Key  |              |
|   | Local ID (optional)                                      |              |
| Copyright & 1998-2001<br>NetScreen Technologies | Preferred Certificate (optional)                         |              |
| All rights received,                            | Local Cert None -  |              |
|   | Peer CA None *   |              |
|   |  |              |
|   | OK Cancel  |              |
|   |  | -            |
| Go to the Gateway Configuration                 | 🔮 brter  | net          |

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: T**oPIX501**المصادقة:** ما **قبل** الآنم**جموعة DH:** المجموعة 2**التشفير:** -3DES CBC**التجزئة: SHA-1العمر الافتراضي:** 3600 بايية

ثانية.

| NetScreen Administration  | i Tools - Microsoft Internet Explorer  | - 8 X            |
|---|--|------------------|
| Ele Edit Yew Favorites  | Jook Heb   | 1 AV             |
| 3 Back • 🕥 - 💌  | 🕄 🐔 🔎 Search 👷 Favortes 😵 Media 🥝 💁 🍃 🗑 - 🌄 🎲  |                  |
| Address 1 http://10.0.3.254   | layout.html*6,1,1  | • 🔂 🐼 🛛 Links 🎽  |
| NETSCREEN-S   | telp support at  | out:      logout |
| System<br>Configure<br>Admin<br>Interface<br>Network<br>Policy<br>VPN<br>Virtual IP<br>Lists<br>Address<br>Service<br>Schedule<br>Users<br>Monitor<br>Traffic<br>Counters<br>Alarm<br>Log | PHASE 1 PROPOSAL CONFIGURATION         Name       ToPb501         Authentication Method       Preshare         DH Group       Group 2 •         Encryption & Data Integrity       SDESCEC •         Hash Algorithm:       SDESCEC •         Lifetime:       * Sec ^ Min ^ Hours ^ Days |                  |
| NetStreen Technologies<br>Inc.<br>All rights pressed  |  |                  |

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

|                             |                   |                        |              | _             |                          |          |  | لتالي.       |
|-----------------------------|-------------------|------------------------|--------------|---------------|--------------------------|----------|--|--------------|
| NetScreen Administratio     | on Tools - Micro  | solt Internet Explorer |              |               |                          |          |  | _ @ X        |
| Ele Edt Yew Favorke         | s Icois Helo      |                        |              |               |                          |          |  |              |
| 🕝 Back + 🕥 - 💌              | 2 🏠 🖇             | Search 👷 Favorite      | is 😽 Media 🌾 | 3 3.31        | ē - 🛄 🍪                  |          |  |              |
| Address 1 http://10.0.3.254 | 4/layout.html*6,1 | ,t :-                  |              |               |                          |          | •  | 🔁 Go Links X |
| NETSCREEN - 5               |                   |                        |              |               |                          | • help   | • support • abou   | t • logout   |
| System                      | VPN               | 1                      |              |               |                          |          | 17 Sept 2  | 003 15:42:19 |
| Configure                   |                   |                        |              |               |                          |          |  |              |
| Admin                       |                   |                        |              |               |                          |          |  | Page 2 of 2  |
| Interface                   |                   |                        |              |               | سينجز يتسب               |          | Section of the sectio |              |
| Naturnek                    | Man               | ual Key 🔰 AutoKey IKE  | Gateway      | P1 Proposal V | 2 Proposal V Certificate | L2TP     | IPPool L   |              |
| Neurork                     |                   |                        |              |               |                          |          |  |              |
| Policy                      |                   |                        |              |               |                          |          |  |              |
| VPN                         |                   |                        |              |               |                          |          |  |              |
| Virtual IP                  |                   | Name                   | Method       | DH Group      | Encrypt/Auth.            | Lifetime | Configure  | 1            |
| Lists                       |                   | dsæg2-3desmidő         | DSAcig       | 2             | 30ES/M05                 | 29800    |  |              |
| Address                     |                   | dia-g2-3des-tha        | DEADO        | 2             | 3DES / SHA               | 29800    |  |              |
| Service<br>Scheckula        |                   | ToP6501                | Preshare     | 2             | 3DES / SHA               | 3600     | Edit-Bemave  |              |
| Users                       |                   |                        |              |               |                          |          |  |              |
| Monitor                     |                   |                        |              |               |                          |          |  |              |
| Traffic                     |                   |                        |              |               |                          |          |  |              |
| Counters                    |                   |                        |              |               |                          |          |  |              |
| Alarm                       |                   |                        |              |               |                          |          |  |              |
| Log                         |                   |                        |              |               |                          |          |  |              |
| Copyright @ 1998-2001       |                   |                        |              |               |                          |          |  |              |
| NetScreen Technologies      |                   |                        |              |               |                          |          |  |              |
| all sight reproved          |                   |                        |              |               |                          |          |  |              |

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:** DH-2 (1024 بت)**خوارزمية التشفير:** -3DES CBC**خوارزمية المصادقة:** 1-SHA**مدى الحياة:** 26400

| NetScreen Administration Teals . Micro   | and Internet Fundame   |  | ئانىة<br>× ھا   |
|--|--|--|-----------------|
| File Edit View Favorites Tools Help  |  |  | RIMITS          |
| 🔾 Back + 🕐 - 💽 🗟 🐔 🔎   | Search 👷 Favorites 🜒 Media 🙆 🍰 🥛 💮   | <mark>_</mark> 3                                 |                 |
| Address 🛃 http://10.0.3.254/layout.html*6,1,                                   | 1  |  | • 🛃 Go Links ** |
| NETSCREEN -S   |  | help     support                                 | bout logout     |
| System PHAS  | E 2 PROPOSAL CONFIGURATION   |  | ¥               |
| Network Policy Vietoal IP Lists Address Survice Schedule Users Monitor Traffic | Name<br>Perfect Forward Secrecy<br>Encapsulation<br><sup>(*)</sup> Encryption (ESP)<br>Encryption Algorithm<br>Authentication Algorithm<br><sup>(*)</sup> Authentication Only (AH)<br>Authentication Algorithm | ToPu501<br>DH Group 2 •<br>3DES-CBC •<br>SHA-1 • |                 |
| Copyright & 1909-2001<br>NetScreen Technologies<br>Inc.<br>Alt achter searced  | Lifetime<br>In Time<br>In Kbytes   | 26400<br>← Sec ← Mm ← Hours ← Days<br>0 Kbytes   |                 |

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

| di + 🕑 - 🖹 😰 🐔 🔎 Search 👷 Favorites 🤫 Media: 🤗 🍰 🖏<br>📵 http://10.0.3.254/kryout.htm/*6,1,1  | · 📙 🕉  |  |  |                               |
|--|--|--|--|-------------------------------|
| http://10.0.3.254/layout.html*6,1,1  | - <u></u> 9  |  |  |                               |
| http://10.0.3.254/kypout.html*6,1,1  |  |  |  |                               |
|  |  |  |  | <u> </u>                      |
| TSCREEN'-5   |  | • help   | • sup  | port 🏾 🌢 about                |
| System VPN   |  |  |  | 17 Sept 20                    |
| Configure  |  |  |  |                               |
| Admin  |  |  |  |                               |
|  |  |  | -  |                               |
| Manual Key V AutoKey IXI V Gateway V P1 Proposal V P2  | Proposal V Certificat  | tes 🔰 L27  | b \Lambda I  | PPool 1                       |
| Network  |  |  |  |                               |
| Delles market  |  |  |  |                               |
|  |  |  |  |                               |
|  |  |  |  |                               |
| VPN  |  |  |  |                               |
| VPN<br>Virtual IP  |  | I sa station   | 1.2  |                               |
| VPN<br>Mitual IP<br>Lists PFS Encap.   | Encrypt/Auth.  | . Lifetime   | Lifesize   | Configure                     |
| VPN<br>Mitual IP<br>Lists nopti-ap-dep-md5 No PFS Escap.<br>Address  | Encrypt/Auth.  | Lifetime   | Lifesize<br>0  | Configure                     |
| VPN<br>Wirtuel IP<br>Lists<br>Address<br>Services<br>Services<br>No PFS ESP<br>No PFS ESP<br>Services<br>Services  | Encrypt/Auth.<br>DES/MOS<br>DES/SHA  | Lifetime   | Lifesize<br>0<br>0   | Configure<br>-<br>-           |
| VPN           Wrbual IP           Lists           Address           Service           Schwickula   | Encrypt/Auth.<br>DES/MOS<br>DES/SHA<br>30ES/MOS  | Lifetime   | Lifesize<br>0<br>0   | Configure<br>-<br>-           |
| VPN<br>Virtual IP<br>Lists<br>Address<br>Service<br>Schodule<br>Users<br>No PFS<br>No PFS<br>ESP<br>No PFS<br>ESP  | Encrypt/Auth.<br>DES/MOG<br>DES/SHA<br>30ES/MOS<br>30ES/SHA  | Lifetime 3900 3900 3900 3900 3900 3900 3900  | Lifesize<br>0<br>0<br>0                                    | Configure<br>-<br>-<br>-      |
| VPN           Mittbal IP           Lists         Norme         PFS         Encap.           Address         nopti-esp-dep.md5         No PFS         ESP           Address         nopti-esp-dep.md5         No PFS         ESP           Service         nopti-esp-dep.md5         No PFS         ESP           Schedule         nopti-esp-3dep.md5         No PFS         ESP           Usions         g2-esp-dep.md5         DH Group 2         ESP   | Encrypt/Auth.<br>DES/M05<br>DES/SHA<br>3DES/M05<br>3DES/SHA<br>DES/M05                                     | Lifetime<br>3000<br>3000<br>3000<br>3000<br>3000   | Lifesize<br>0<br>0<br>0<br>0                               | Configure<br>-<br>-<br>-<br>- |
| VPN           Virtual IP           Lists         Name         PFS         Encap.           Address         noptilesp-desination         No PFS         ESP           Address         noptilesp-desination         No PFS         ESP           Scholdule         noptilesp-desination         No PFS         ESP           User/s         noptilesp-desination         No PFS         ESP           Monitor         g2-esp-desination         DH Group 2         ESP           Totalistic         DH Group 2         ESP   | Encrypt/Auth.<br>DES/M06<br>DES/SHA<br>30ES/M06<br>30ES/SHA<br>DES/M06<br>0ES/SHA                          | Lifetime<br>3900<br>3900<br>3900<br>3900<br>3900<br>3900   | Lifesize<br>0<br>0<br>0<br>0<br>0                          | Configure<br>-<br>-<br>-<br>- |
| VPN       Wrtual IP       Lists       Address       Address       Service       Schodula       Users       Monitor       Traffic       Character       Schodula       DH Group 2       ESP       Schodula       District       Schodula       District       Schodula       Difficience       Schodula   | Encrypt/Auth.<br>DES/M06<br>DES/SHA<br>30ES/M05<br>30ES/SHA<br>DES/SHA<br>0ES/SHA<br>30ES/M05              | <ul> <li>Lifetime</li> <li>3900</li> </ul> | Lifesize<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0           | Configure<br>                 |
| VPN       Mittbal IP       Lists       Address       Address       Service       Schodule       Usins       Usins       Monitor       If affic       Counters       Q2-exp-desmd5       DH Group 2       ESP       Schodule       No PFS       ESP       Monitor       g2-exp-desmd5       DH Group 2       ESP       Schodbard       Schodbard       DH Group 2       ESP       Schodbard       Schodbard       Schodbard  | Encrypt/Auth.<br>DES/MOS<br>DES/SHA<br>3DES/MOS<br>3DES/SHA<br>DES/MOS<br>DES/SHA<br>3DES/MOS<br>3DES/SHA  | Lifetime<br>3900<br>3900<br>3900<br>3900<br>3900<br>3900<br>3900<br>390  | Lifesize<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0 | Configure<br>                 |
| VPN       Mittbal IP       Lists       Address       Service       Schodule       Users       Schodule       Users       Monitor       If affic       Counters       S2-exp-desmd5       DH Group 2       ESP       Schodule       Users       Schodule       Users       S2-exp-desmd5       DH Group 2       ESP       S2-exp-desmd5       DH Group 2       ESP <t< td=""><td>Encrypt/Auth.<br/>DES/MOS<br/>DES/SHA<br/>3DES/MOS<br/>3DES/SHA<br/>DES/MOS<br/>3DES/SHA<br/>3DES/SHA<br/>3DES/SHA</td><td>Lifetime<br/>3900<br/>3900<br/>3900<br/>3900<br/>3900<br/>3900<br/>3900<br/>390</td><td>Lifesize<br/>0<br/>0<br/>0<br/>0<br/>0<br/>0<br/>0<br/>0<br/>0<br/>0</td><td>Configure<br/></td></t<> | Encrypt/Auth.<br>DES/MOS<br>DES/SHA<br>3DES/MOS<br>3DES/SHA<br>DES/MOS<br>3DES/SHA<br>3DES/SHA<br>3DES/SHA | Lifetime<br>3900<br>3900<br>3900<br>3900<br>3900<br>3900<br>3900<br>390  | Lifesize<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0 | Configure<br>                 |

- 11. حدد علامة التبويب **AutoKey IKE،** ثم انقر فوق **إدخال IKE AutoKey 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:** 1-VPN**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.)

| NetScreen Administratio  | n Tools - Microsoft Internet Explorer   |
|--|---|
| Ele Edit Yew Favorites   | Tools Help  |
| 🔇 Back + 🚫 - 💌   | 💈 🐔 🔎 Search 👷 Favorites 🜒 Media 🥝 🍰 🤤 🐨 🛄 🦓  |
| Address ) http://10.0.3.254  | Anyout. Heni <sup>46</sup> 6,1,1 🔹 🛃 Go Unida 🏁   |
| NETSCREEN'-5   | help     is support     is about  |
| System<br>Configure<br>Admin   | AUTOKEY IKE CONFIGURATION   |
| Interface<br>Network<br>Policy<br>VPN<br>Virtual IP<br>Lists<br>Address<br>Service | Name VPN-1<br>Enable Replay Protection T Enable<br>Remote Gateway Tunnel Name To501 V Ust Gateways<br>Phase 2 Proposal ToFtx501 V |
| Schedule<br>Users<br>Monitor<br>Traffic<br>Counters                                | none<br>Lut Phase 2 Proposis<br>VPN Monitor ♥ Enable<br>Transment Mide ♥ Enable   |
| Copyright © 1990-2001<br>NetScreen Technologies<br>Inc.                            | Cancel  |

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

| NetScreen Administratio     | m Tools - Micro  | soft Interne   | t Explorer    |                   |                       |                |                   |                 | _           | 5)   |
|-----------------------------|------------------|----------------|---------------|-------------------|-----------------------|----------------|-------------------|-----------------|-------------|------|
| Ele Edit Yew Favorite       | s Icols Help     |                |               |                   |                       |                |                   |                 |             | a,   |
| 🕒 Back • 🕥 · 🛓              | 3 🖒 🖇            | Search 5       | Favorites 🚷   | Meda 🙆            | 🕱 • 😓 🖩 • 🚺           | 3              |                   |                 |             |      |
| Address 1 http://10.0.3.254 | (layout.html*6,1 | ,1             |               |                   |                       |                |                   | •               | 🔁 Go 🛛 Lini | ks X |
| NETSCREEN'-5                |                  |                |               |                   |                       |                | • hilp •          | support • about | • logou     | t.   |
| System                      | VPN              |                |               |                   |                       |                |                   | 17 Sept 20      | 003 15:46:0 | 06   |
| Configure                   |                  |                |               |                   |                       |                |                   |                 | 2.5.4       |      |
| Admin                       |                  |                |               |                   |                       |                |                   |                 | Page 1 of   | 1    |
| Interface                   | TRU              |                | ANT OF LAST   |                   |                       | Contraction of | 1070              | IPPool          |             |      |
| Network                     | - Mari           | ual key 😈 A    | novel ive A C | ateway 🖞 Pi       | Proposal V P2 Proposa | Certificates   |                   | IPP001          |             |      |
| Policy                      |                  | Concernance of |               | Sector Collection |                       |                | and the second of |                 | e i         |      |
| VPN                         |                  | Name           | Gateway       | Replay            | P2 Proposals          | Monitor        | Transport         | Configure       |             |      |
| Virtual IP                  |                  | VPN-1          | To501         | No                | ToPix501              | On             | Off               | · Rds           |             |      |
| Lists                       |                  |                |               |                   |                       |                |                   |                 |             |      |
| Address                     |                  |                |               |                   |                       |                |                   |                 |             |      |
| Service                     |                  |                |               |                   |                       |                |                   |                 |             |      |
| Schedule                    |                  |                |               |                   |                       |                |                   |                 |             |      |
| Users                       |                  |                |               |                   |                       |                |                   |                 |             |      |
| Monitor                     |                  |                |               |                   |                       |                |                   |                 |             |      |
| Traffic                     |                  |                |               |                   |                       |                |                   |                 |             |      |
| Counters                    |                  |                |               |                   |                       |                |                   |                 |             |      |
| Alarm                       |                  |                |               |                   |                       |                |                   |                 |             |      |
| Log                         |                  |                |               |                   |                       |                |                   |                 |             |      |
| Copyright @ 1998-2001       |                  |                |               |                   |                       |                |                   |                 |             |      |
| NetScreen Technologies      |                  |                |               |                   |                       |                |                   |                 |             |      |
| all order present           |                  |                |               |                   |                       |                |                   |                 |             |      |

- 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: VPN1 (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.)

| NetScreen Administration Tools - Microsoft Internet Explorer | _16/×   |
|--|---|
| Elle Edit View Favorites Icols Help                          | 2   |
| 🔇 Back + 🕗 - 🖹 🗟 🏠 🔎 Search 👷 Favorites 🔮 Media 🤗            | 👶 - 😓 📾 - 🔂 🍇   |
| Address A http://10.0.3.254/layout.html*6,1,1                | 🛫 🛃 Go Unis **  |
| NETSCREEN'-5   | Interpret in the support in the |
| System POLICY CONFIGURATION                                  |   |
| Configure  |   |
| Interface  |   |
| Network Name (optional)                                      |   |
| Policy Source Address  | i InsideNetwork 💌   |
| Vertual IP Destination Address                               | RemoteNetwork 💌   |
| Lists Service  | ANY   |
| Address NAT  | r 🤊 Off   |
| Scherfuls  | C DIP OF  |
| Users  | C DIP On  |
| Monitor  |   |
| Artien   | Tunnel ×  |
| Alarm VPN Tunnel   | VPN1 •  |
| Log  | Modify matching incoming VPN solicy   |
| Cepyright © 1993-2001  | None -  |
| he. All first means  |   |

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.



## <u>التحقق من الصحة</u>

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

### <u>أوامر التحقق</u>

تدعم <u>أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر</u> 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.

#### <u>ناتج التحقق</u>

يتم عرض نموذج الإخراج من **أوامر ping** وshow 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
.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<116ms TTL=128
Reply from 10.0.25.1: bytes=32 time<110ms 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<110ms TTL=128
Reply from 10.0.25.1: bytes=32 time<118ms TTL=128
Reply from 10.0.25.1: bytes=32 time<118ms TTL=128
```

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\_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 <u>معلومات مهمة حول أوامر التصحيح</u> 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
                                       TSAKMP:
                                                   auth pre-share
                                            life type in seconds
                                 ISAKMP:
                                   life duration (basic) of 28800
                       ISAKMP:
                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
                                                  : 1
                                      type
                                                 : 17
                                     protocol
                                                : 500
                                    port
                                      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
      TSAKMP:
                  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
```

#### <u>معلومات ذات صلة</u>

- مفاوضة IPSec/بروتوكولات IKE
  - برنامج جدار حماية <u>Cisco PIX</u>
- <u>مراجع أوامر جدار حماية PIX الآمن من Cisco</u>
- <u>الإعلامات الميدانية لمنتج الأمان (بما في ذلك PIX)</u>
  - <u>طلبات التعليقات (RFCs)</u>
  - الدعم التقني والمستندات <u>Cisco Systems</u>

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما