تكوين PIX إلى طاقة Cisco Secure VPN Client Wild-Card، مشترك مسبقا، no mode-config

المحتويات

المقدمة

يوضح هذا التكوين كيفية توصيل عميل VPN بجدار حماية PIX باستخدام أحرف البدل والأوامر المتوافقة مع **IPSec** و**sysopt IPsec**. يغطي هذا المستند أيضا أمر **nat 0 access-list**.

ملاحظة: تخضع تكنولوجيا التشفير لضوابط التصدير. من مسؤوليتك معرفة القانون المتعلق بتصدير تقنية التشفير. إذا كانت لديك أية أسئلة متعلقة بالتحكم في التصدير، فعليك إرسال بريد إلكتروني إلى export@cisco.com.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- برنامج Cisco Secure PIX الإصدار 5.0.3 مع Cisco Secure VPN Client 1.0 (يظهر على هيئة 2.0.7 في قائمة التعليمات > حول) أو Cisco Secure PIX Software الإصدار 6.2.1 مع Cisco Secure VPN Client

1.1 (يظهر على هيئة 2.1.12 في قائمة التعليمات > حول).
- تصل أجهزة الإنترنت إلى مضيف الويب الموجود بالداخل باستخدام عنوان IP 192.68.0.50.
- يقوم عميل شبكة VPN بالوصول إلى جميع الأجهزة الموجودة بالداخل باستخدام جميع المنافذ (10.1.1.0 /24 و 10.2.2.0 /24).

تم إنشاء المعلومات المُقدمة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كنت تعمل في شبكة مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى اصطلاحات تلميحات Cisco التقنية.

معلومات أساسية

على ال PIX، **ال access-list** و**nat 0** يعمل أمر معا. يتم نويت الأمر **nat 0 access-list** أن يكون استعملت بدلا من الأمر pl **sysopt ips متوافق**. إن يستعمل أنت ال **nat 0** أمر مع ال يماثل **منفذ قائمة** أمر، أنت يضطر عرفت العنوان من الزبون أن يجعل ال VPN توصيل in order to خلقت ال يماثل منفذ تحكم قائمة (ACL) أن يتجاوز ال NAT.

ملاحظة: يتم تطوير الأمر **sysopt ipSec متوافق مع pl** بشكل أفضل من الأمر **nat 0** مع الأمر **access-list** المطابق لتخطي ترجمة عنوان الشبكة (NAT). السبب هو أنك لا تحتاج إلى معرفة عنوان IP الخاص بالعملاء الذين يجعلون الاتصال. الأوامر القابلة للتبديل جريئة في التكوين في هذا المستند.

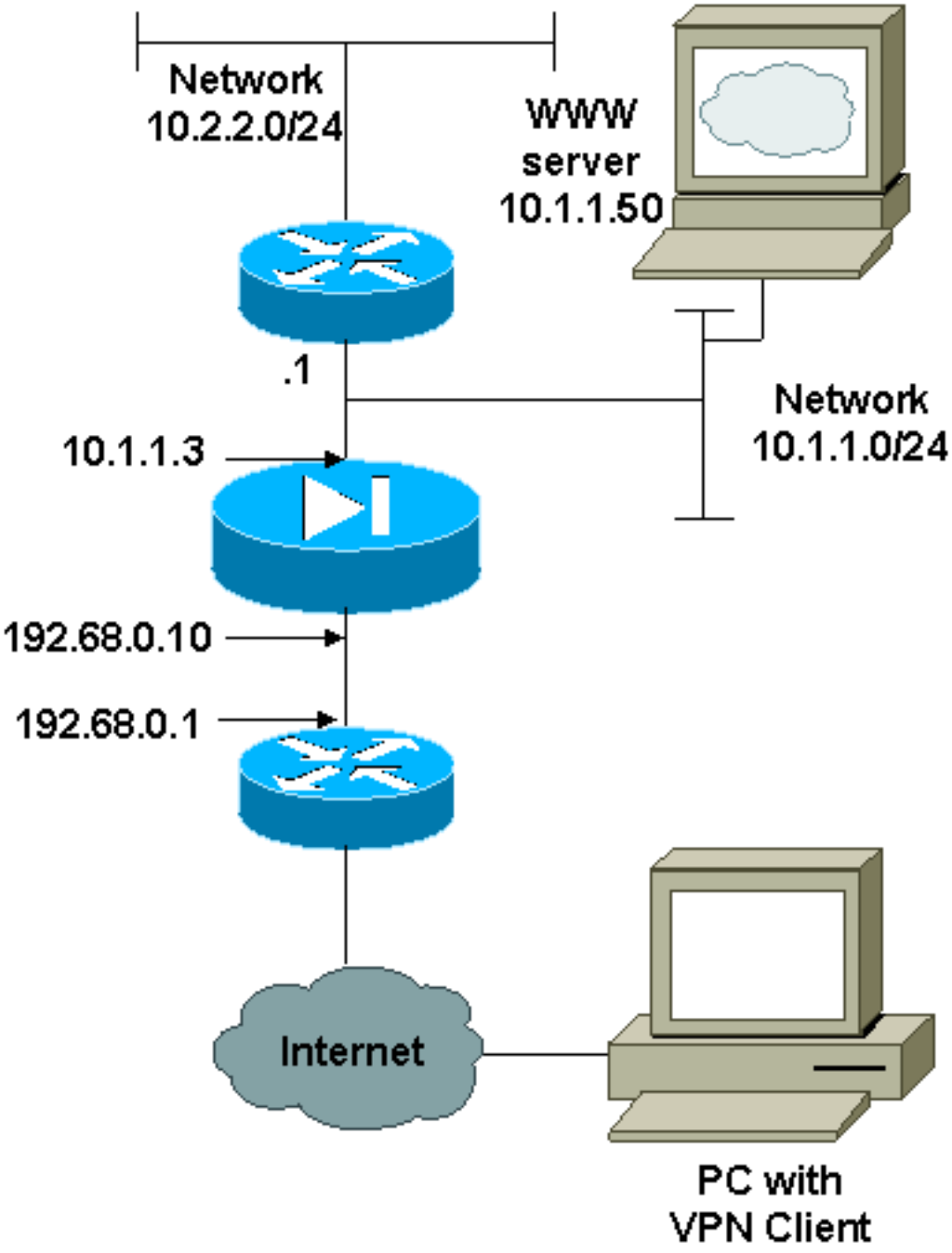
يتصل مستخدم لديه عميل شبكة VPN بعنوان IP ويستلمه من موفر خدمة الإنترنت (ISP) الخاص به. يمكن للمستخدم الوصول إلى كل شيء موجود بداخل جدار الحماية. وهذا يشمل الشبكات. كما يمكن للمستخدمين الذين لا يقومون بتشغيل العميل الاتصال بخادم ويب باستخدام العنوان الذي تم توفيره بواسطة التعيين الثابت. يمكن للمستخدمين في الداخل الاتصال بالإنترنت. ليس من الضروري أن تمر حركة مرور البيانات عبر نفق IPSec.

التكوين

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

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة الموضح في هذا الرسم التخطيطي.



التكوينات

يستخدم هذا المستند التكوينات الموضحة هنا.

- PIX
- عميل شبكة VPN

تكوين PIX

```
PIX Version 6.2.1
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
fixup protocol ftp 21
fixup protocol http 80
```

```
fixup protocol smtp 25
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol sqlnet 1521
names
The ACL to bypass the NAT. You have to know the !-- ---!
    - IP address of the Client. In this case, it is !---
subnet 65.10.10.0/24. access-list 103 permit ip 10.0.0.0
255.0.0.0 65.10.10.0 255.255.255.0
pager lines 24
no logging timestamp
no logging standby
logging console debugging
no logging monitor
no logging buffered
no logging trap
logging facility 20
logging queue 512
interface ethernet0 10baset
interface ethernet1 auto
mtu outside 1500
mtu inside 1500
ip address outside 192.68.0.10 255.255.255.0
ip address inside 10.1.1.3 255.255.255.0
no failover
failover timeout 0:00:00
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
arp timeout 14400
global (outside) 1 192.68.0.11-192.168.0.15 netmask
255.255.255.0
Binding ACL 103 to the NAT statement in order to !- ---!
-- avoid NAT on the IPSec packet. nat (inside) 0 access-
list 103
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
static (inside,outside) 192.68.0.50 10.1.1.50 netmask
255.255.255.255 0 0
conduit permit icmp any any
no rip outside passive
no rip outside default
no rip inside passive
no rip inside default
route outside 0.0.0.0 0.0.0.0 192.68.0.1 1
route inside 10.2.2.0 255.255.255.0 10.1.1.1 1
timeout xlate 3:00:00 conn 1:00:00 half-closed 0:10:00
udp 0:02:00
timeout rpc 0:10:00 h323 0:05:00
timeout uauth 0:05:00 absolute
+aaa-server TACACS+ protocol tacacs
aaa-server RADIUS protocol radius
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
The sysopt ipsec pl-compatible command !--- avoids ---!
    conduit on the IPSec encrypted traffic. !--- This
command needs to be used if you do not use !--- the nat
.0 access-list command

sysopt ipsec pl-compatible
sysopt connection permit-ipsec
crypto ipsec transform-set myset esp-des esp-md5-hmac
crypto dynamic-map cisco 1 set transform-set myset
crypto map dyn-map 20 ipsec-isakmp dynamic cisco
```

```
crypto map dyn-map interface outside
isakmp enable outside
isakmp key cisco123 address 0.0.0.0 netmask 0.0.0.0
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 1
isakmp policy 10 lifetime 1000
telnet timeout 5
terminal width 80
Cryptochecksum:c687aa0afb1dd03abce04c31566b5c52
end :
[OK]
```

تكوين عميل شبكة VPN

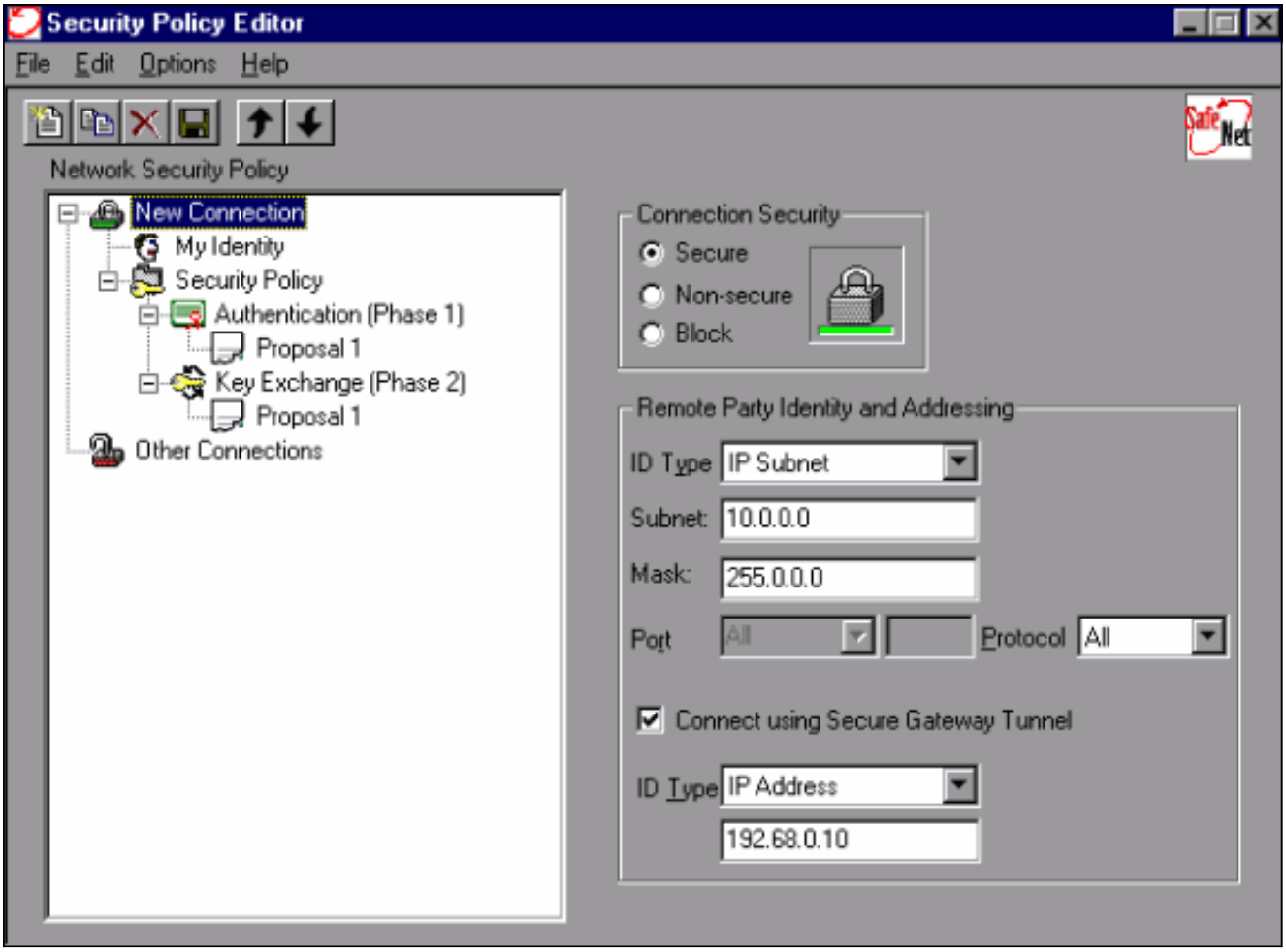
```
:Network Security policy
TACconn 1-
My Identity
Connection security: Secure
Remote Party Identity and addressing
ID Type: IP subnet
10.0.0.0
255.0.0.0
Port all Protocol all

Connect using secure tunnel
ID Type: IP address
192.68.0.10

(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
```

تكوين نهج اتصال IPSec لعميل VPN

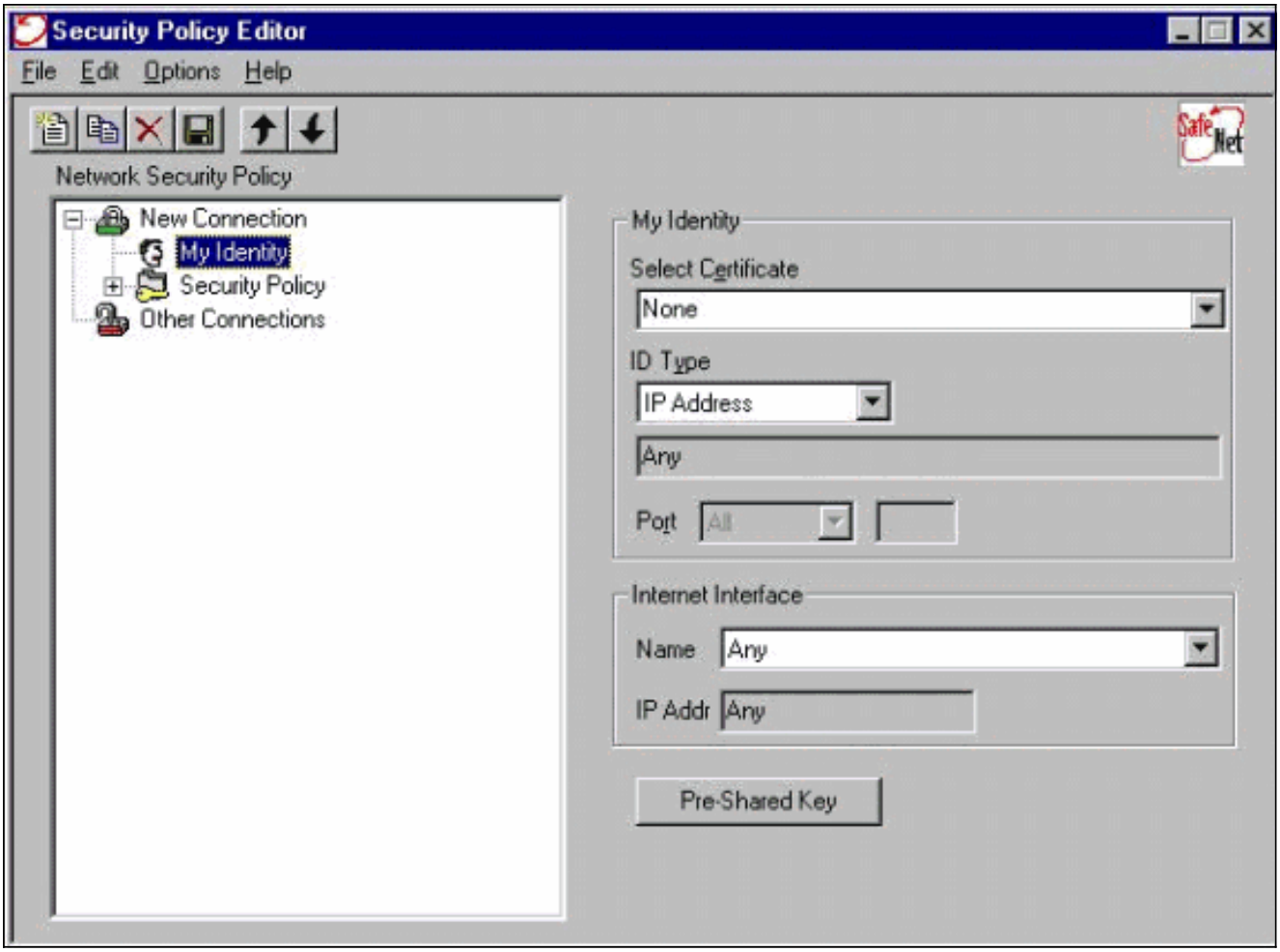
اتبع هذه الخطوات لتكوين النهج لاتصال IPSec لعميل VPN.

1. في علامة التبويب "هوية الطرف البعيد والعنونة"، قم بتحديد الشبكة الخاصة التي تريد الوصول إليها باستخدام

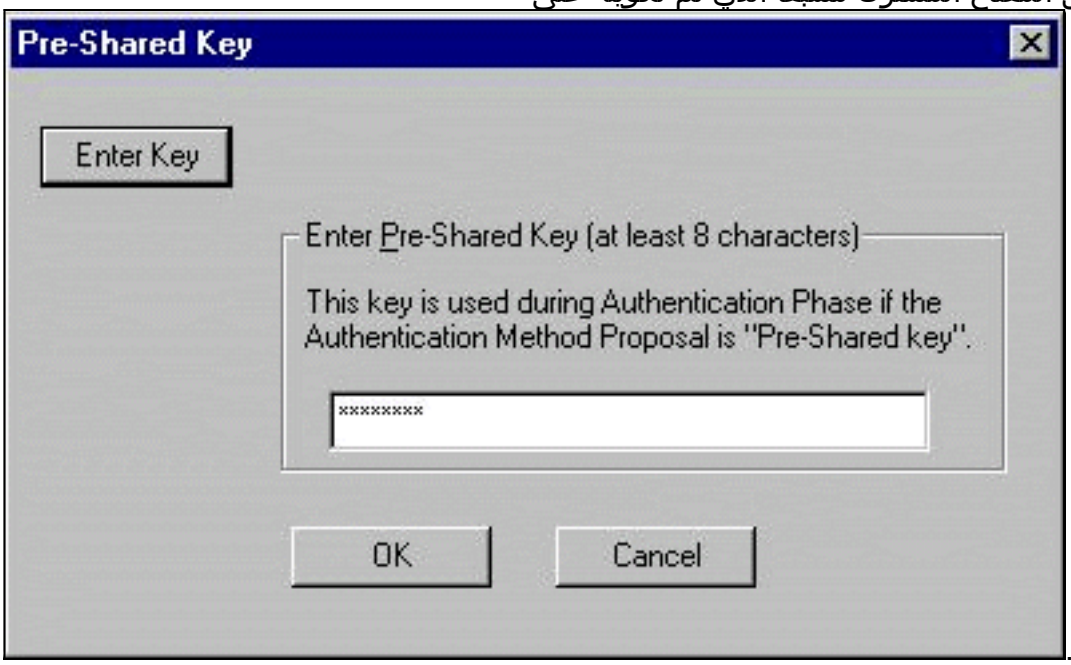
عميل شبكة VPN. بعد ذلك، حدد **اتصال باستخدام نفق العبارة الآمنة** وحدد عنوان IP الخارجي ل PIX.



2. حدد **هويتي** واترك الإعداد إلى الإعداد الافتراضي. بعد ذلك، انقر على زر **مفتاح مشترك مسبقا**.

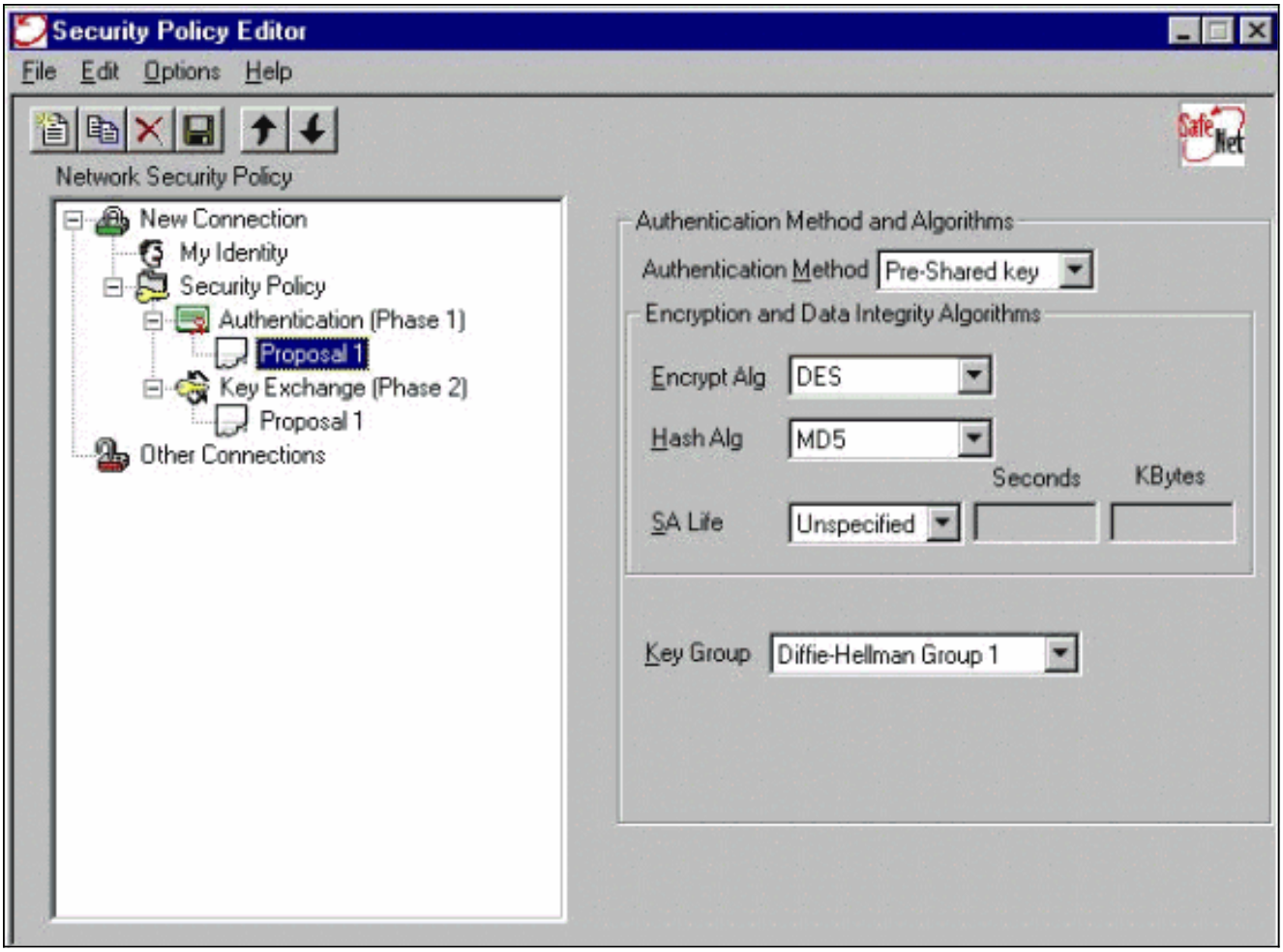


3. أدخل المفتاح المشترك مسبقا الذي تم تكوينه على

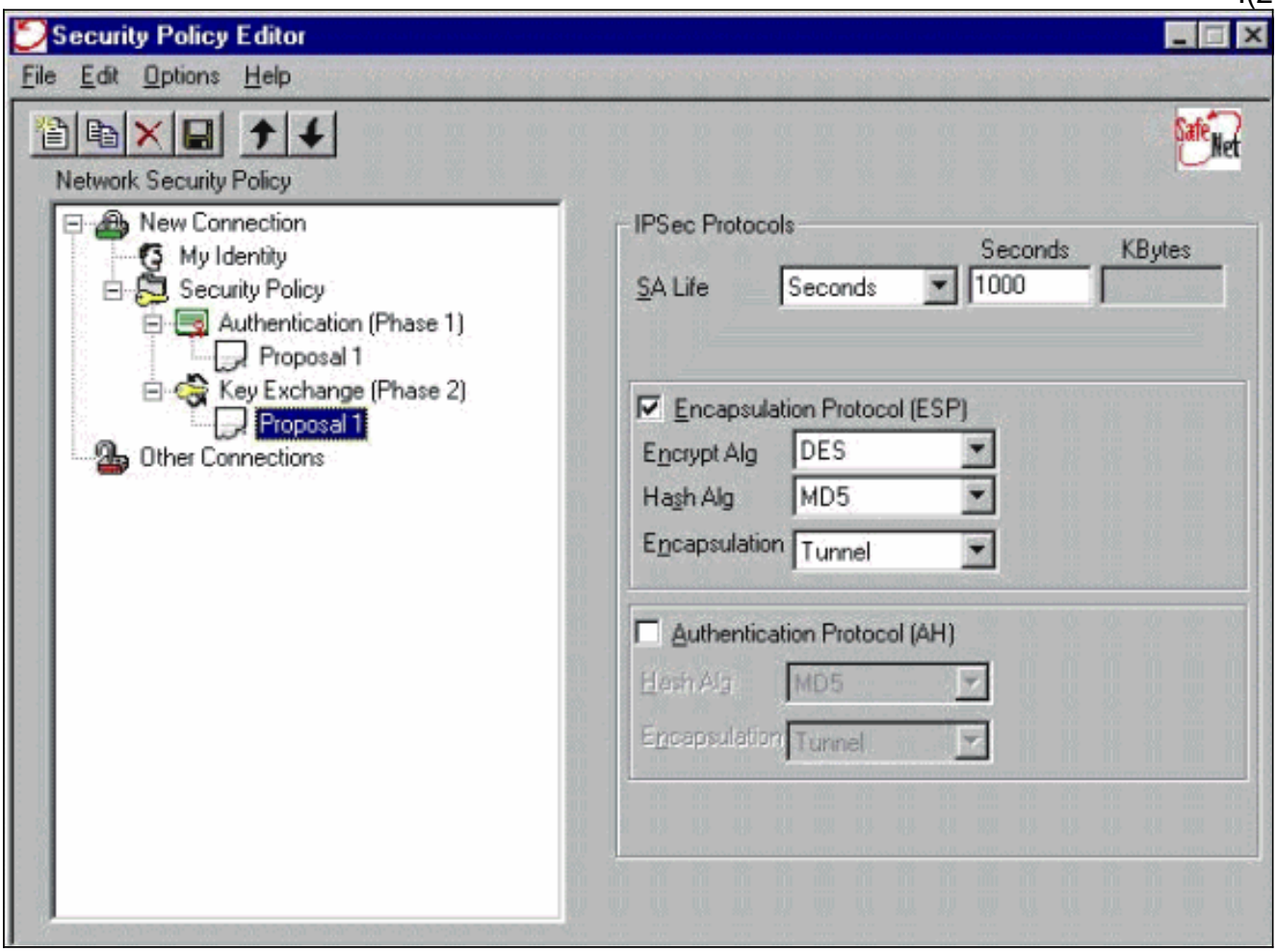


.PIX

4. تكوين مقترح المصادقة (نهج المرحلة 1).



5. تكوين اقتراح IPSec (سياسة المرحلة 2).



ملاحظة: لا تنس حفظ النهج عند الانتهاء. افتح نافذة DOS وأزيز مضيف معروف على الشبكة الداخلية ل PIX لبدء النفق من العميل. تتلقى رسالة يتعذر الوصول إليها إلى بروتوكول رسائل التحكم في الإنترنت (ICMP) من عملية إختبار الاتصال الأولى أثناء محاولة التفاوض على النفق.

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 debug

ملاحظة: قبل إصدار أوامر **debug**، راجع المعلومات المهمة في أوامر تصحيح الأخطاء.

لعرض تصحيح أخطاء جانب العميل، قم بتمكين عارض السجل الآمن من Cisco:

- **debug crypto ipSec** - يعرض مفاوضات IPSec للمرحلة 2.
- **debug crypto isakmp sa** - يعرض مفاوضات ISAKMP للمرحلة 1.
- **debug crypto Engine** - يعرض الجلسات المشفرة.

معلومات ذات صلة

- مراجع أوامر جدار حماية PIX الآمن من Cisco
- الإعلامات الميدانية لمنتج الأمان (بما في ذلك PIX)
- دعم منتج برنامج جدار حماية Cisco PIX
- طلبات التعليقات (RFCs)
- صفحات دعم منتجات أمان IP (IPSec)
- تكوين أمان شبكة IPSec
- تكوين بروتوكول أمان Internet Key Exchange
- مقدمة عن تشفير أمان IP (IPSec)
- الاتصال من خلال جدار حماية PIX
- تكوين IPSec
- 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).