تكوين IPSec بين خادم Microsoft Windows 2000 وجهاز Cisco

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين نفق IPSec بمفاتيح مشتركة مسبقا للانضمام إلى شبكتين خاصتين: شبكة خاصة (I.X.192.168) داخل جهاز Cisco وشبكة خاصة (X.10.32.50) داخل خادم Microsoft 2000. نفترض أن حركة المرور من داخل جهاز Cisco وداخل خادم 2000 إلى الإنترنت (ممثلة هنا بشبكات X.172.18.124) تتدفق قبل بدء هذا التكوين.

يمكنك العثور على معلومات تفصيلية حول تكوين خادم Microsoft Windows 2000 في موقع Microsoft على الويب: http://support.microsoft.com/support/kb/articles/Q252/7/35.ASP

قبل البدء

الاصطلاحات

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

المتطلبات الأساسية

لا توجد متطلبات أساسية خاصة لهذا المستند.

المكونات المستخدمة

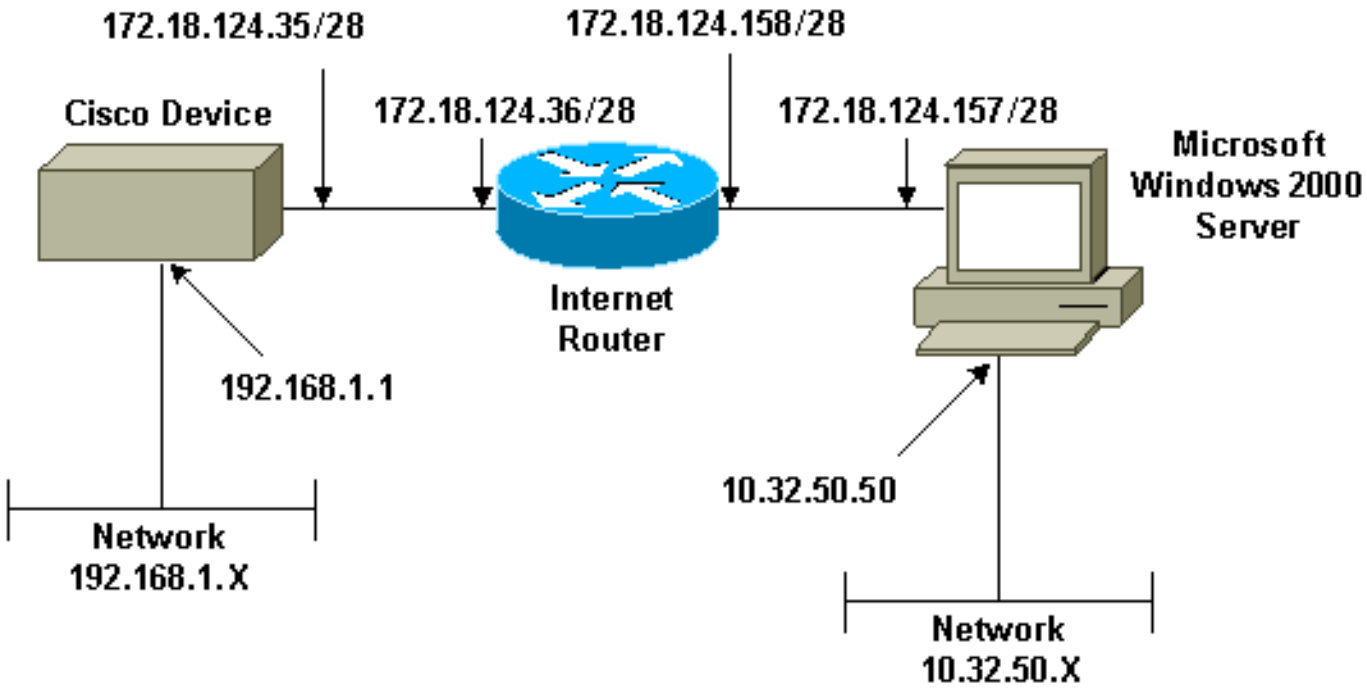
تم تطوير هذه المواصفات واختبارها باستخدام إصدارات البرامج والأجهزة أدناه.

- Microsoft Windows 2000 Server 5.00.2195
- cisco 3640 مسحاج تخديد مع cisco ios ® برمجية إطلاق c3640-ik2o3s-mz.121-5.T.bin
- جدار حماية PIX الآمن من Cisco مع برنامج PIX، الإصدار 5.2.1
- مركز Cisco VPN 3000 مع برنامج مركز VPN 3000 نسخة F.2.5.2
- مركز Cisco VPN 5000 مع برنامج مركز VPN 5000 نسخة 5.2.19

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 قبل استخدامه.

الرسم التخطيطي للشبكة

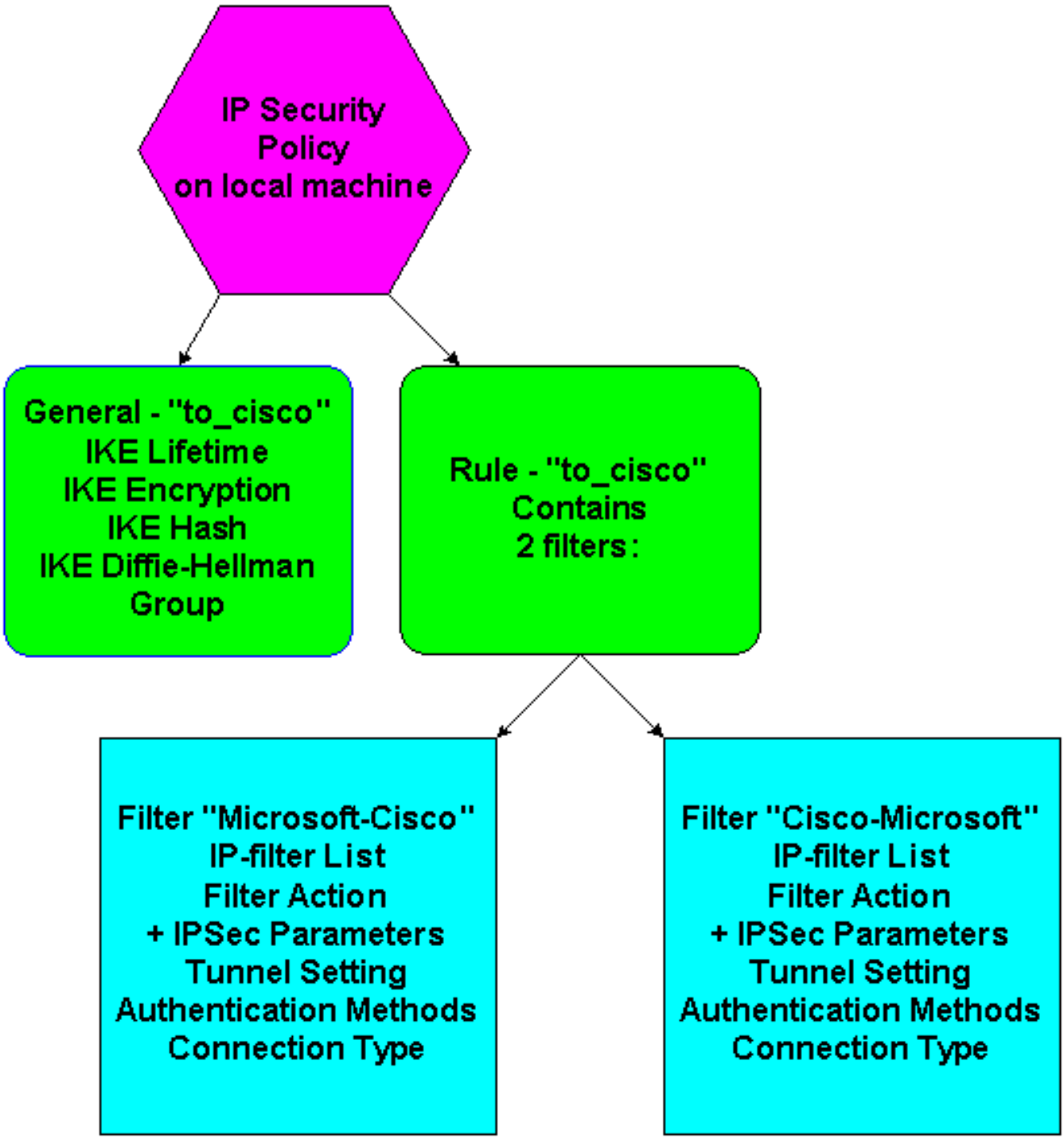
يستخدم هذا المستند إعداد الشبكة الموضح في الرسم التخطيطي أدناه.



تكوين خادم Microsoft Windows 2000 للعمل باستخدام أجهزة Cisco

المهام التي تم تنفيذها

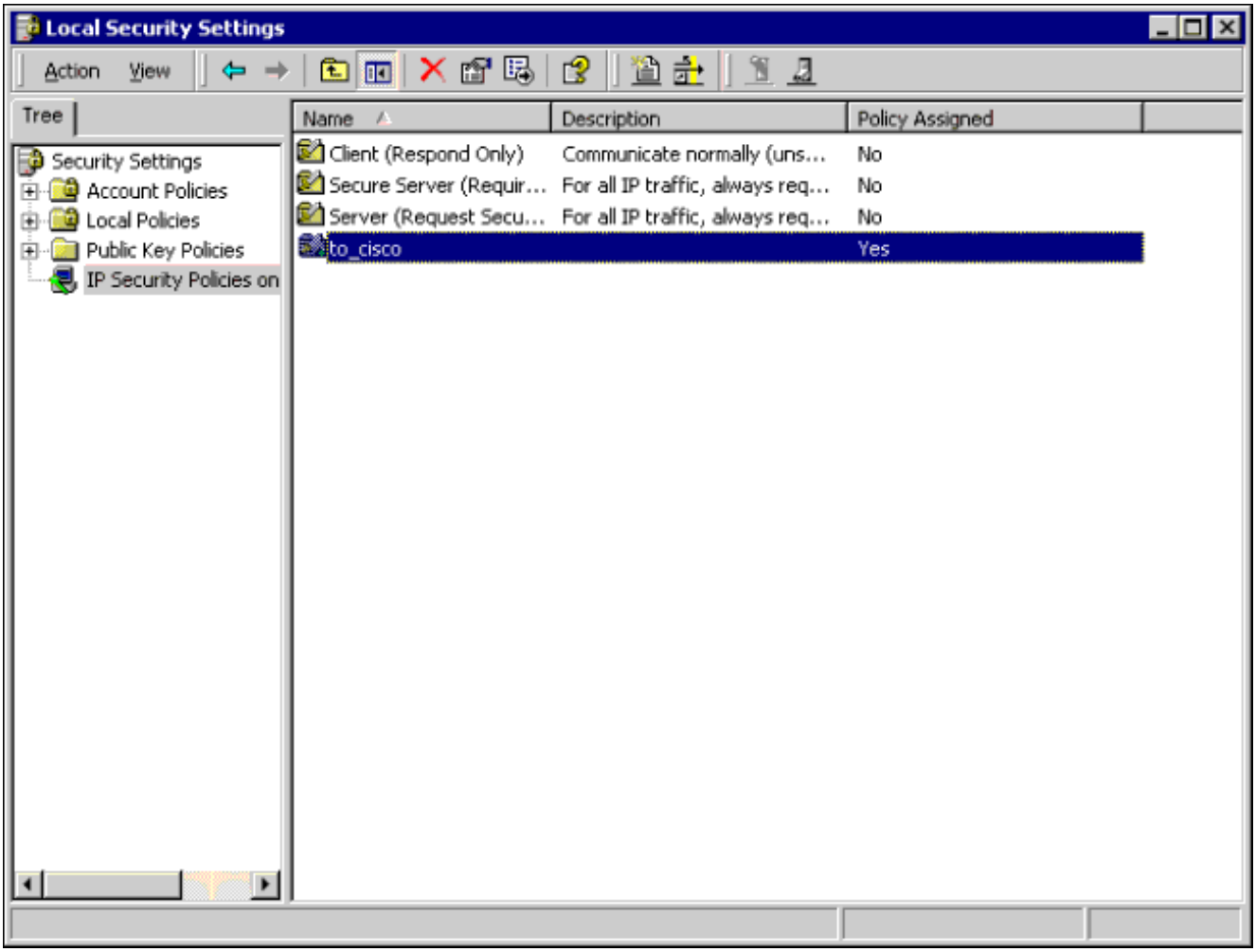
يوضح هذا المخطط المهام التي تم تنفيذها في تكوين خادم Microsoft Windows 2000:



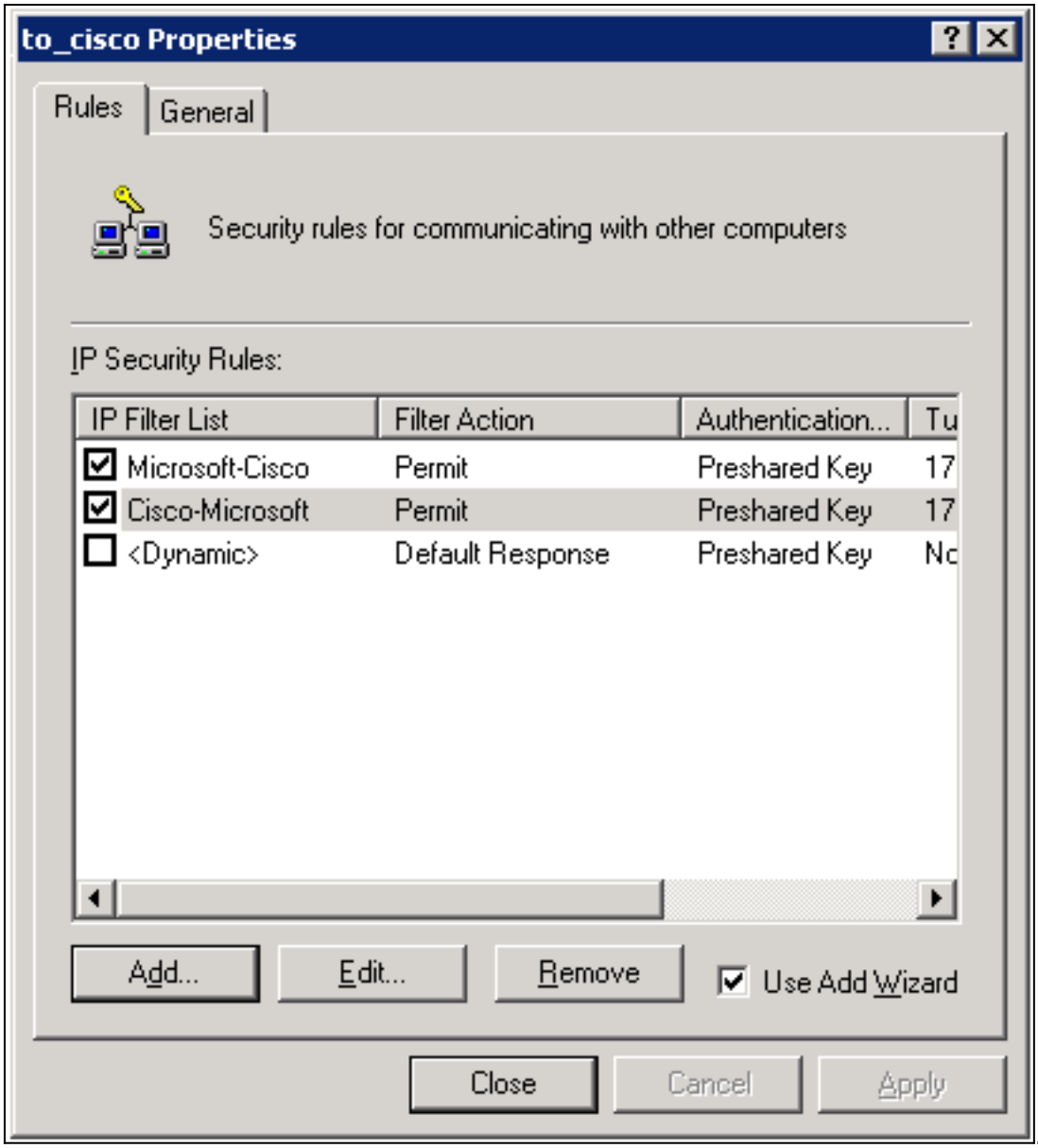
التعليمات بالتفصيل

بمجرد اتباع إرشادات التكوين على موقع Microsoft على الويب، أستخدم الخطوات التالية للتحقق من إمكانية عمل التكوين الخاص بك مع أجهزة Cisco. يتم ملاحظة التعليقات والتغييرات باستخدام لقطات الشاشة.

1. انقر على **ابدأ > تشغيل > secpol.msc** على Microsoft Windows 2000 Server، وتحقق من المعلومات على الشاشات التالية.بعد إستخدام الإرشادات الموجودة على موقع Microsoft على ويب لتكوين خادم 2000، تم عرض معلومات النفق التالية.**ملاحظة:** تسمى قاعدة المثال "to_cisco".

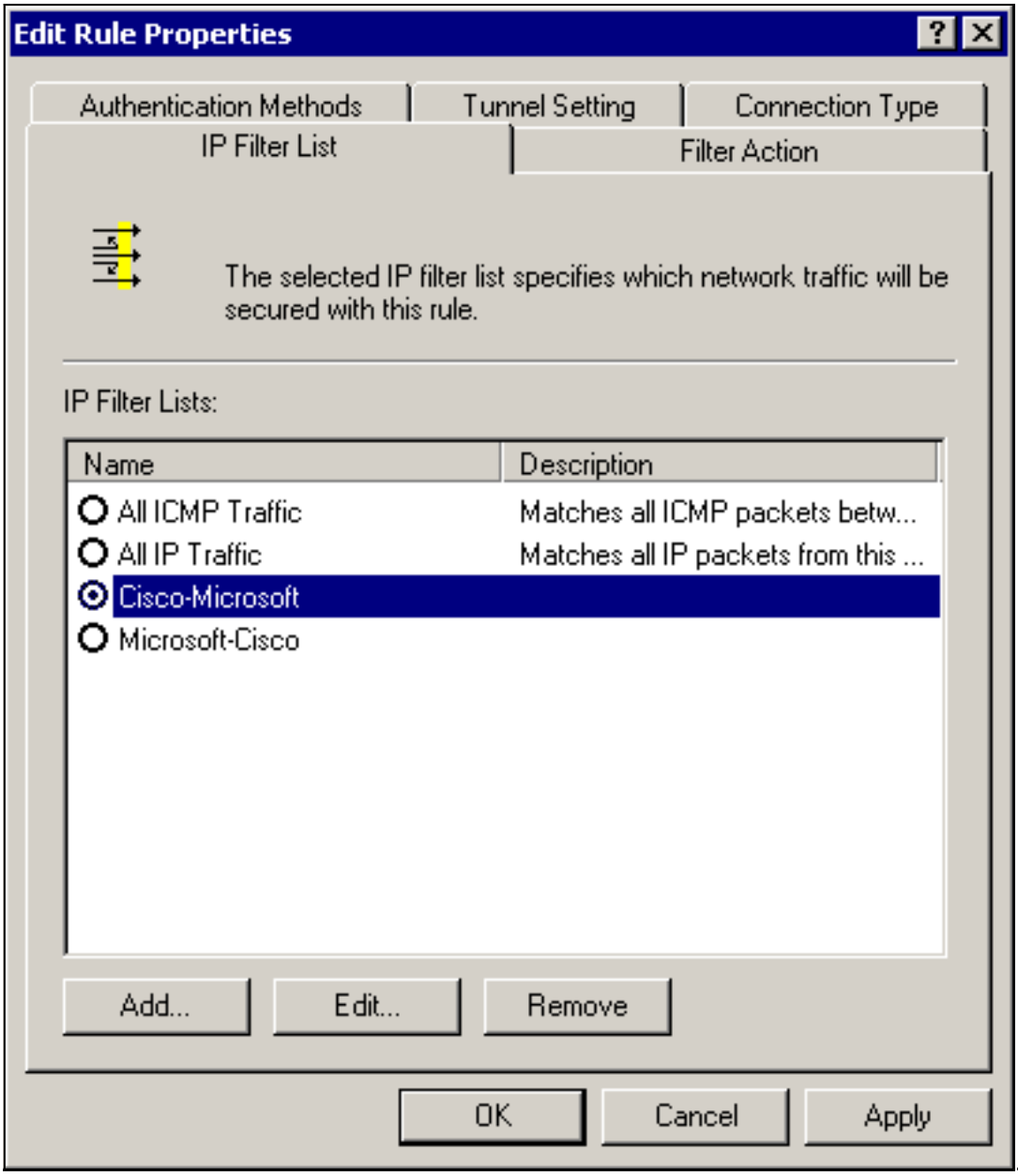


2. تحتوي قاعدة المثال هذه على عوامل تصفية: Microsoft-Cisco و -Cisco



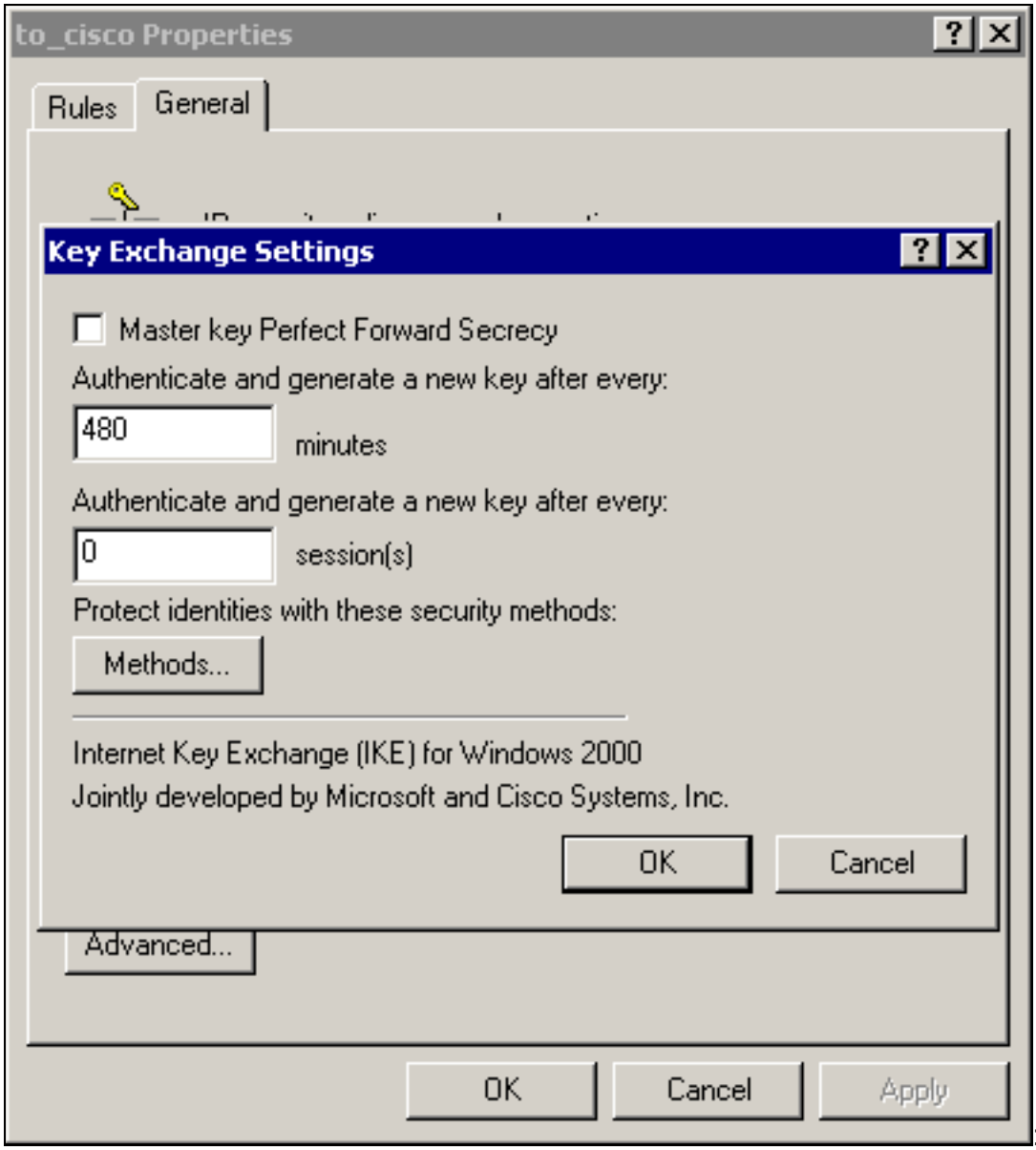
Microsoft.

3. حدد قاعدة أمان Cisco-Microsoft IP، ثم انقر فوق **تحرير** لعرض/إضافة/تحرير قوائم عوامل تصفية



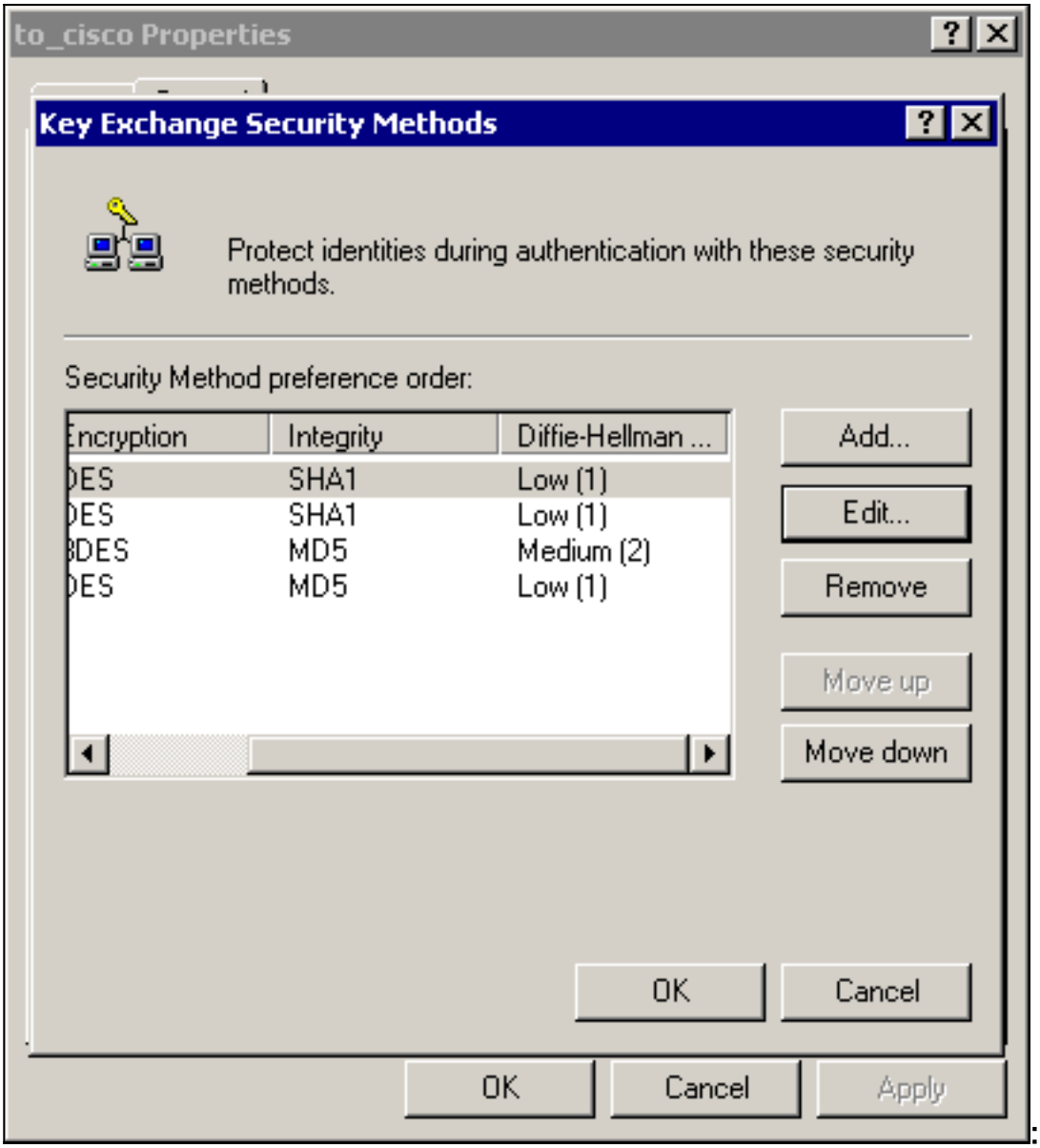
.IP

4. تحتوي علامة التبويب **عام** للقاعدة > **خيارات متقدمة** على **العمر الافتراضي ل** 480) **IKE** دقيقة = 28800



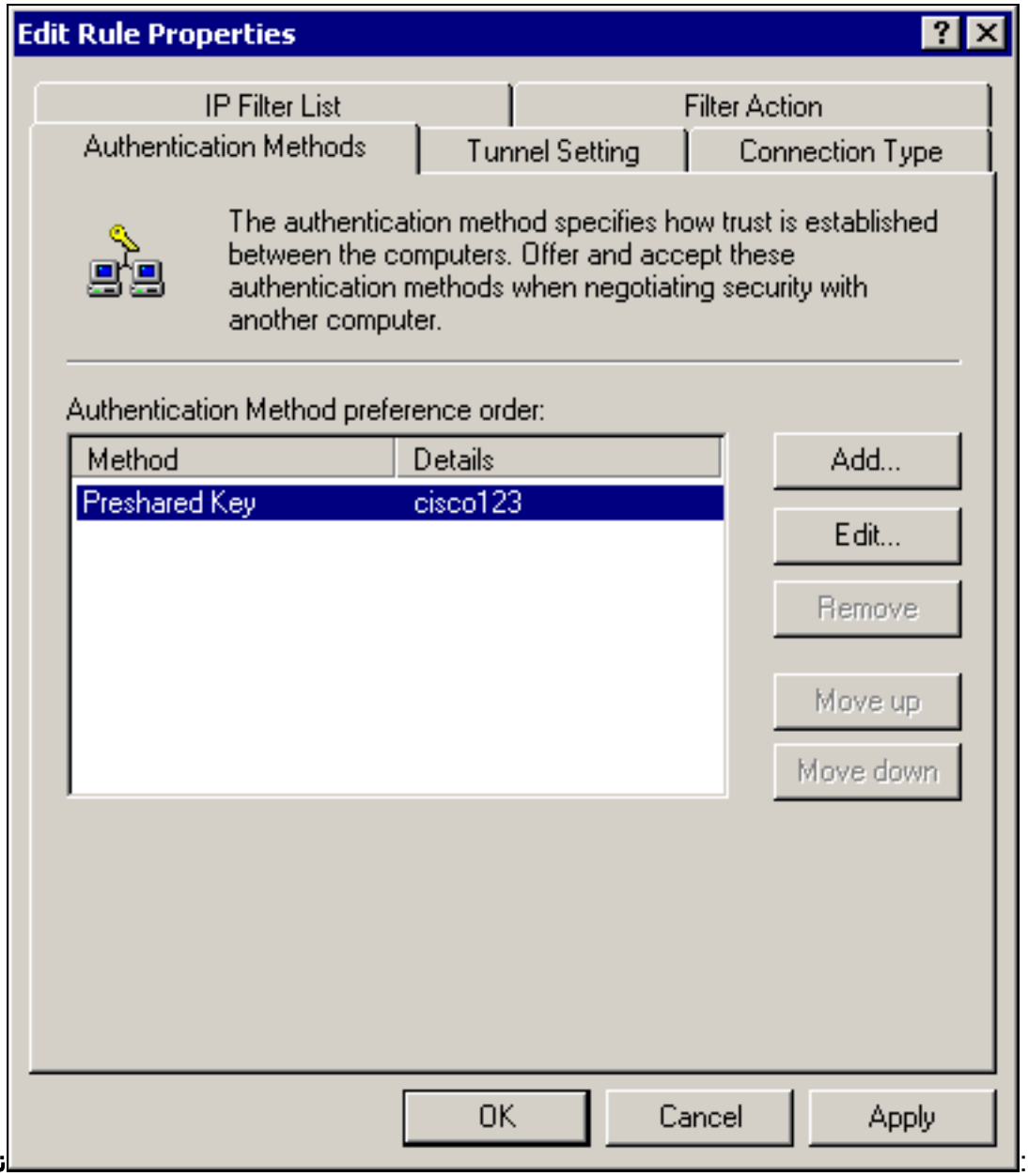
ثانية):

5. تتضمن علامة التبويب **عام** للقاعدة > **خيارات متقدمة** > **أساليب** أسلوب **تشفير** IKE (DES) و**تجزئة IKE** (SHA1)) ومجموعة **Diffie-Helman**

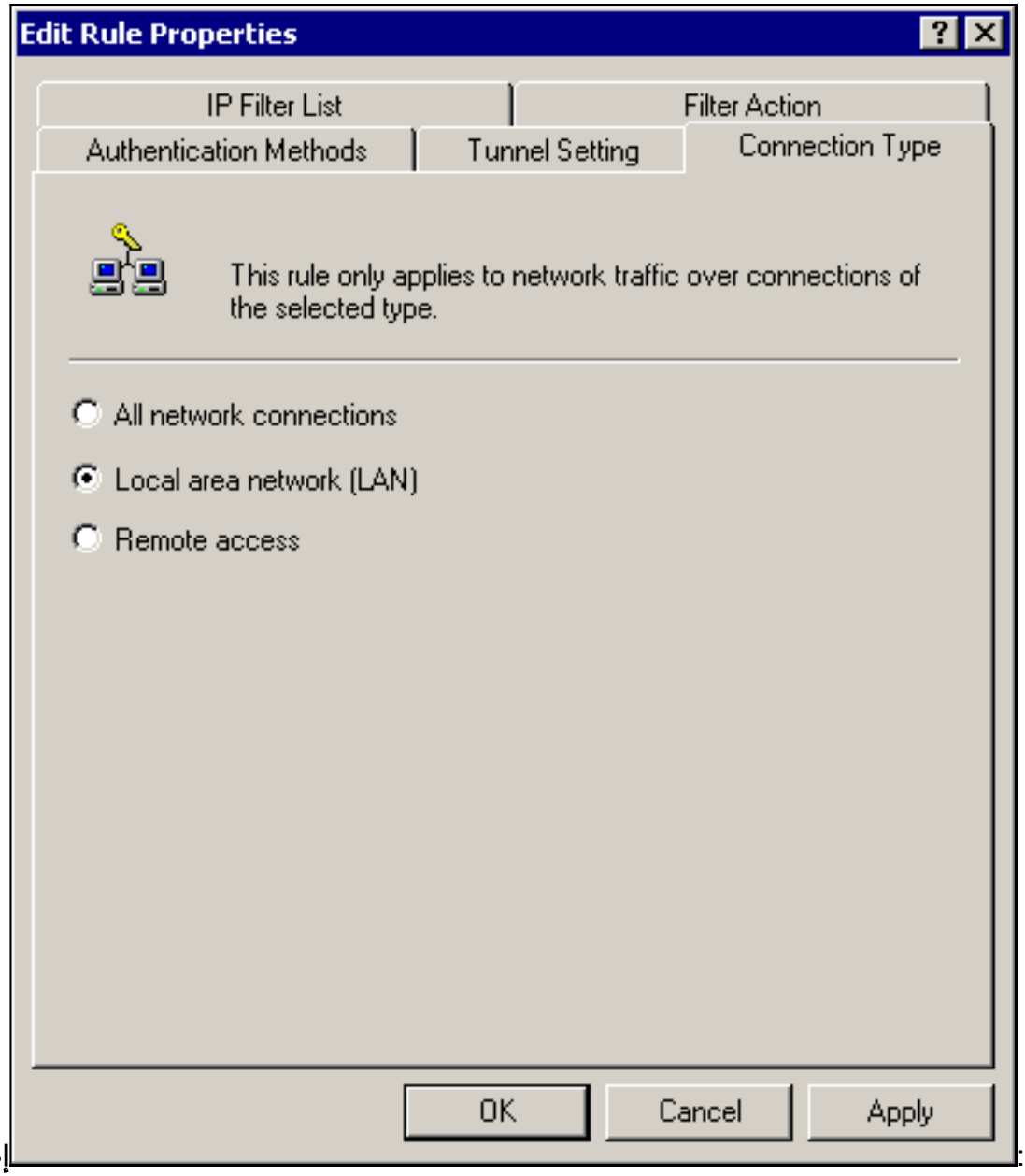


(**منخفضة(1)**):

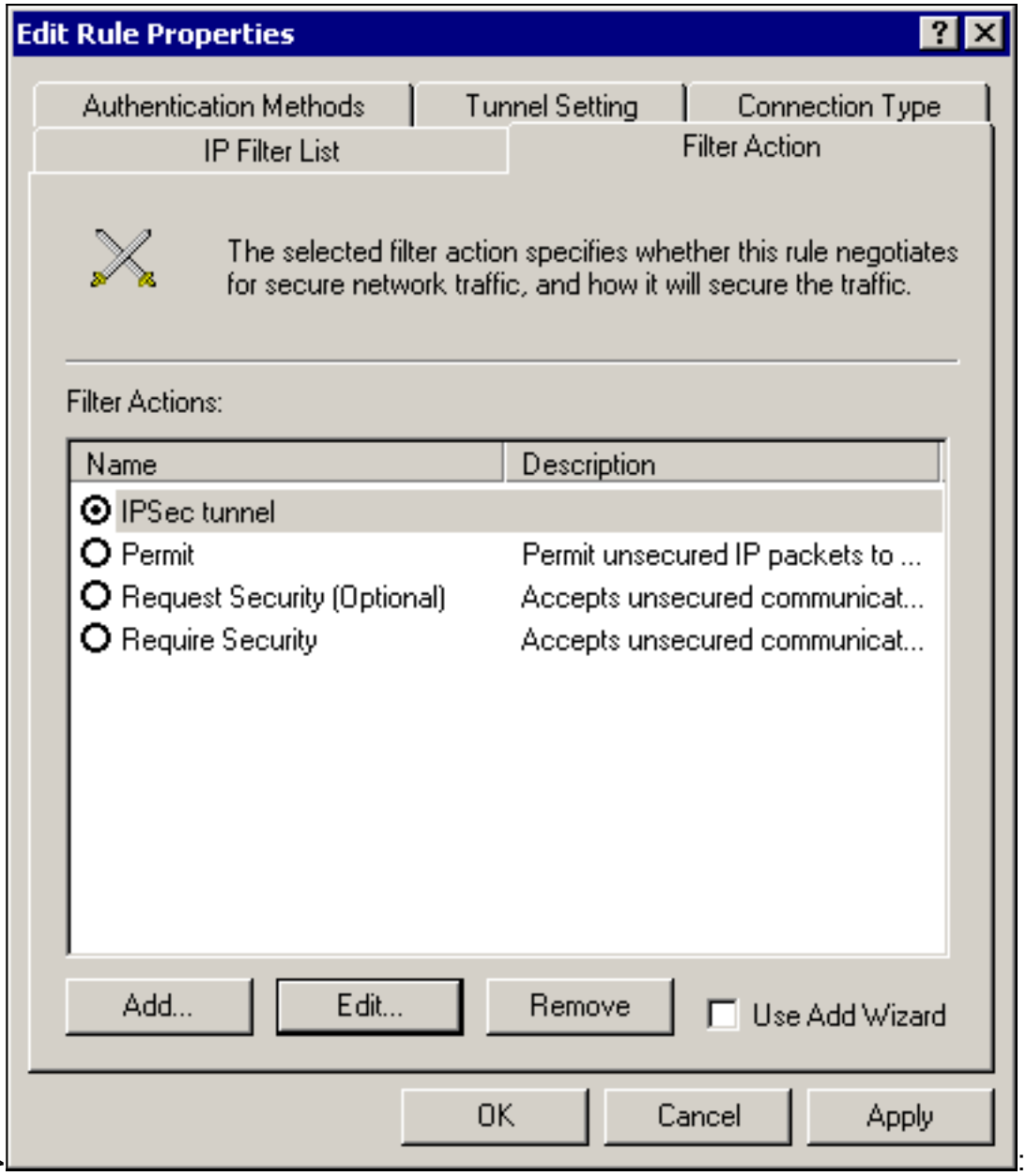
6. يحتوي كل عامل تصفية على 5 علامات تبويب:**أساليب المصادقة** (المفاتيح المشتركة مسبقا لتبادل مفتاح الإنترنت



نوع الاتصال:([IKE]

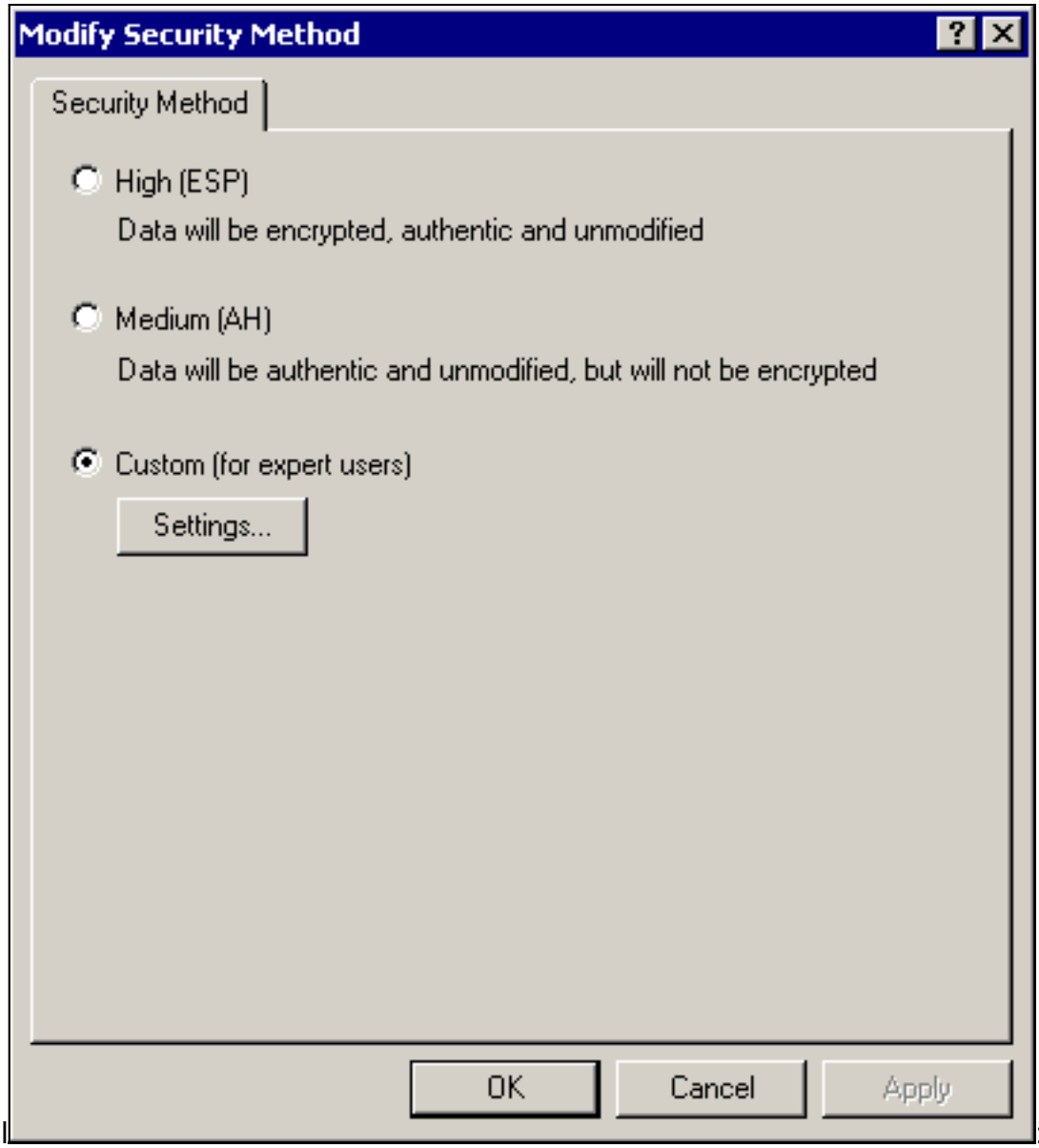


إجراء التصفية:(LAN)



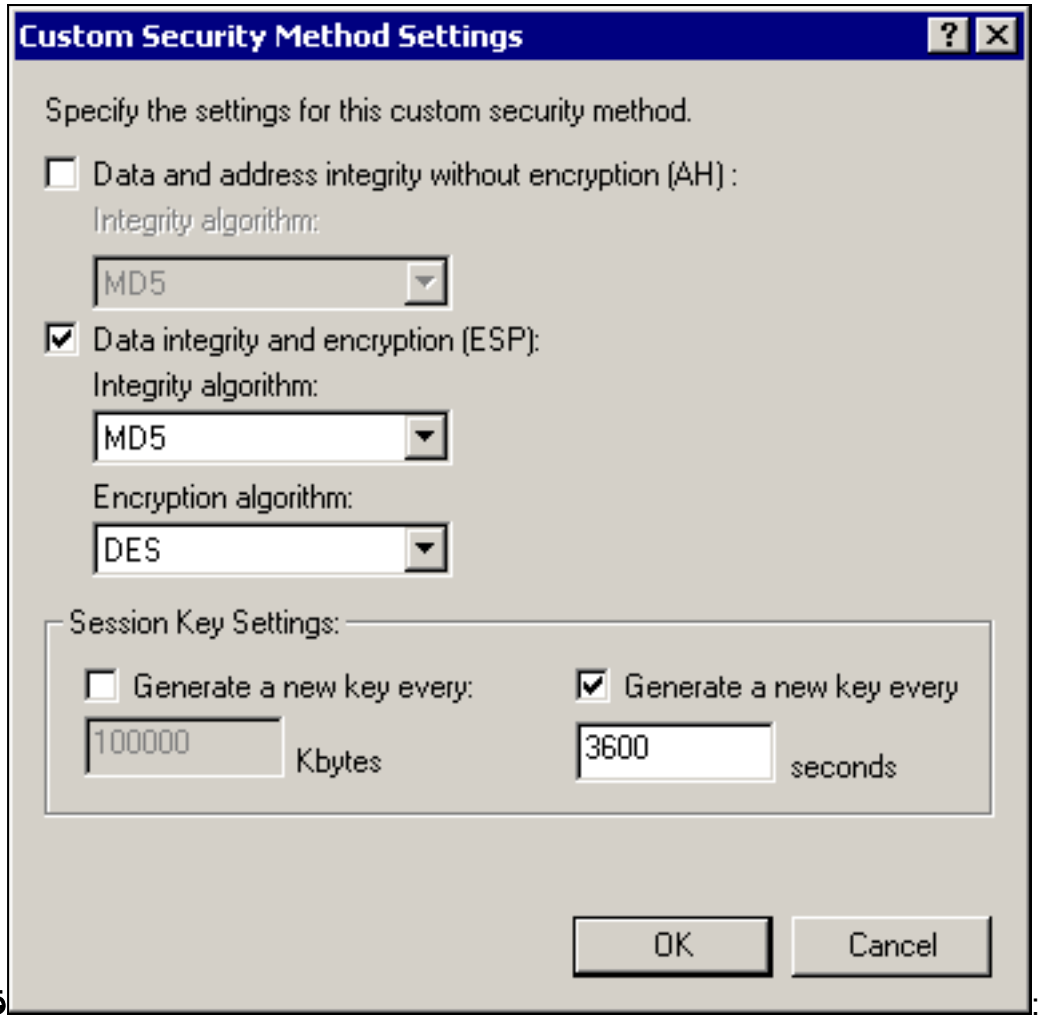
حدد **عملية** (IPSec):

التصفية > نفق IPSec > تحرير > تحرير، وانقر



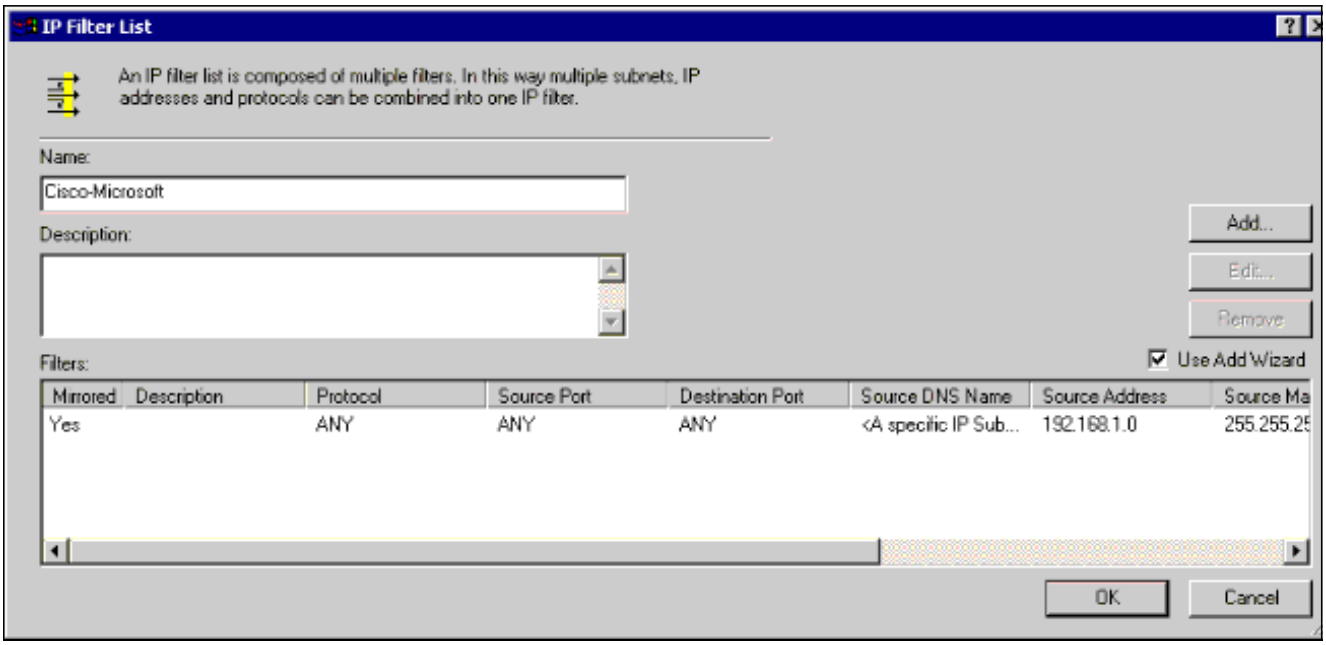
انقر فوق **مخصص**:

الإعدادات - عمليات تحويل IPSec وفترة بقاء

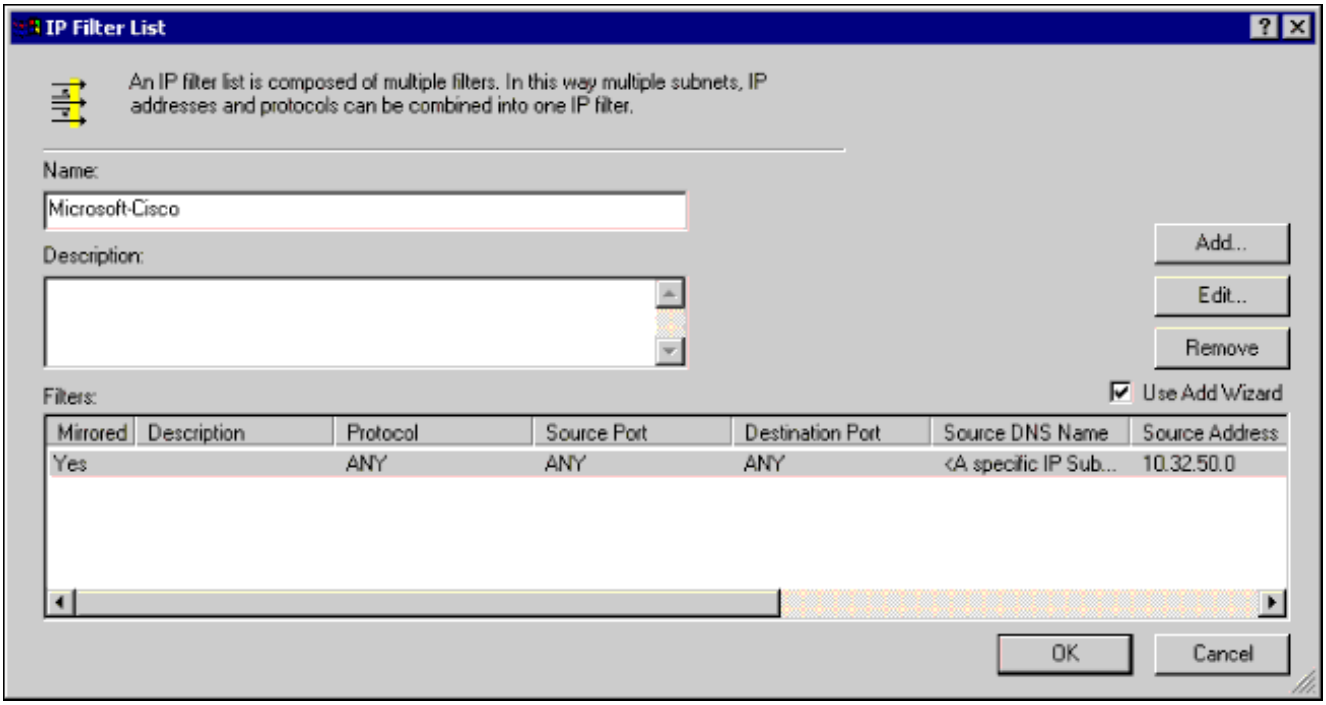


قائمة عوامل IPSec:

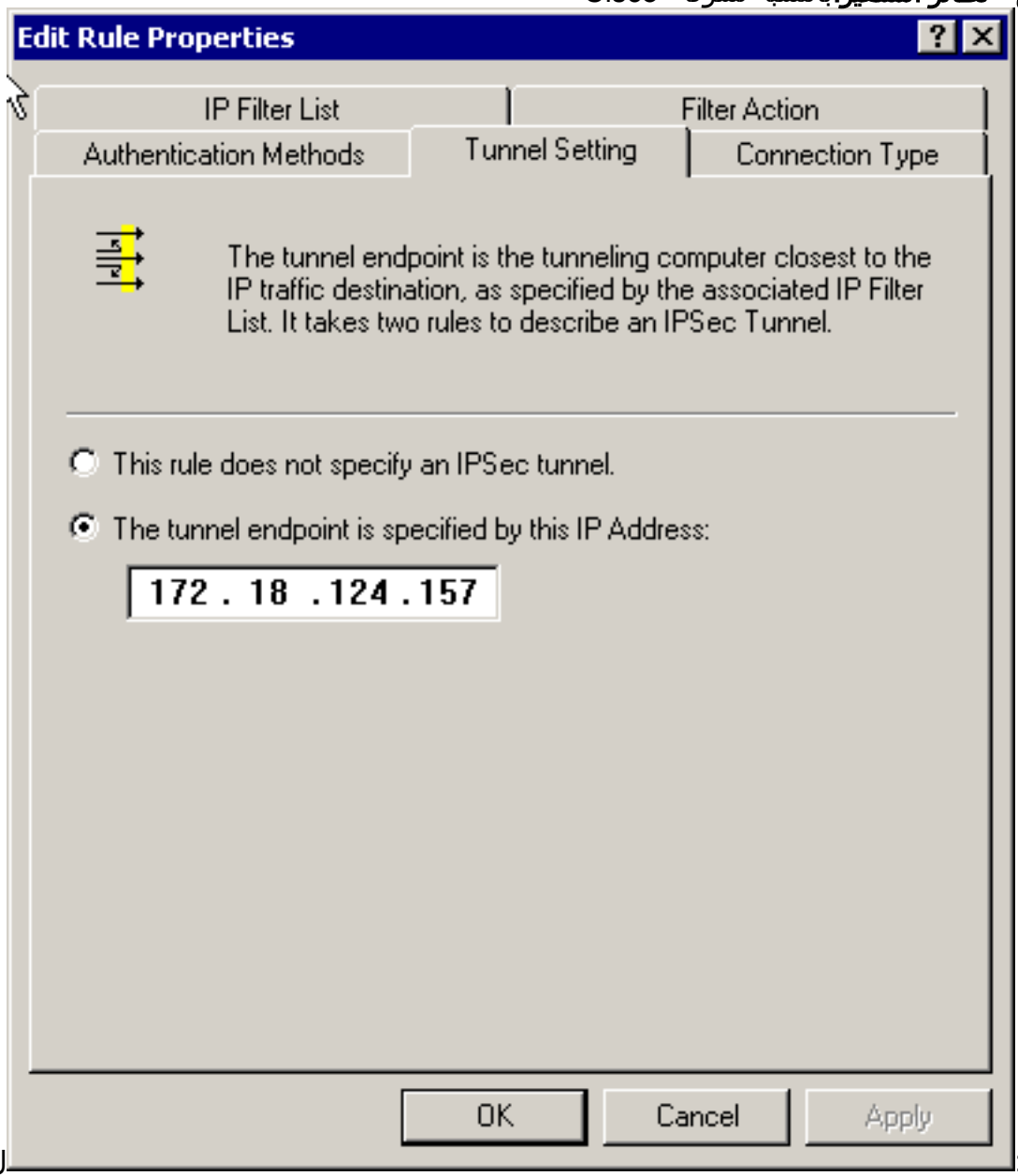
تصفية IP - شبكات المصدر **والوجهة** المطلوب تشفيرها:بالنسبة لشركة Cisco-Microsoft:



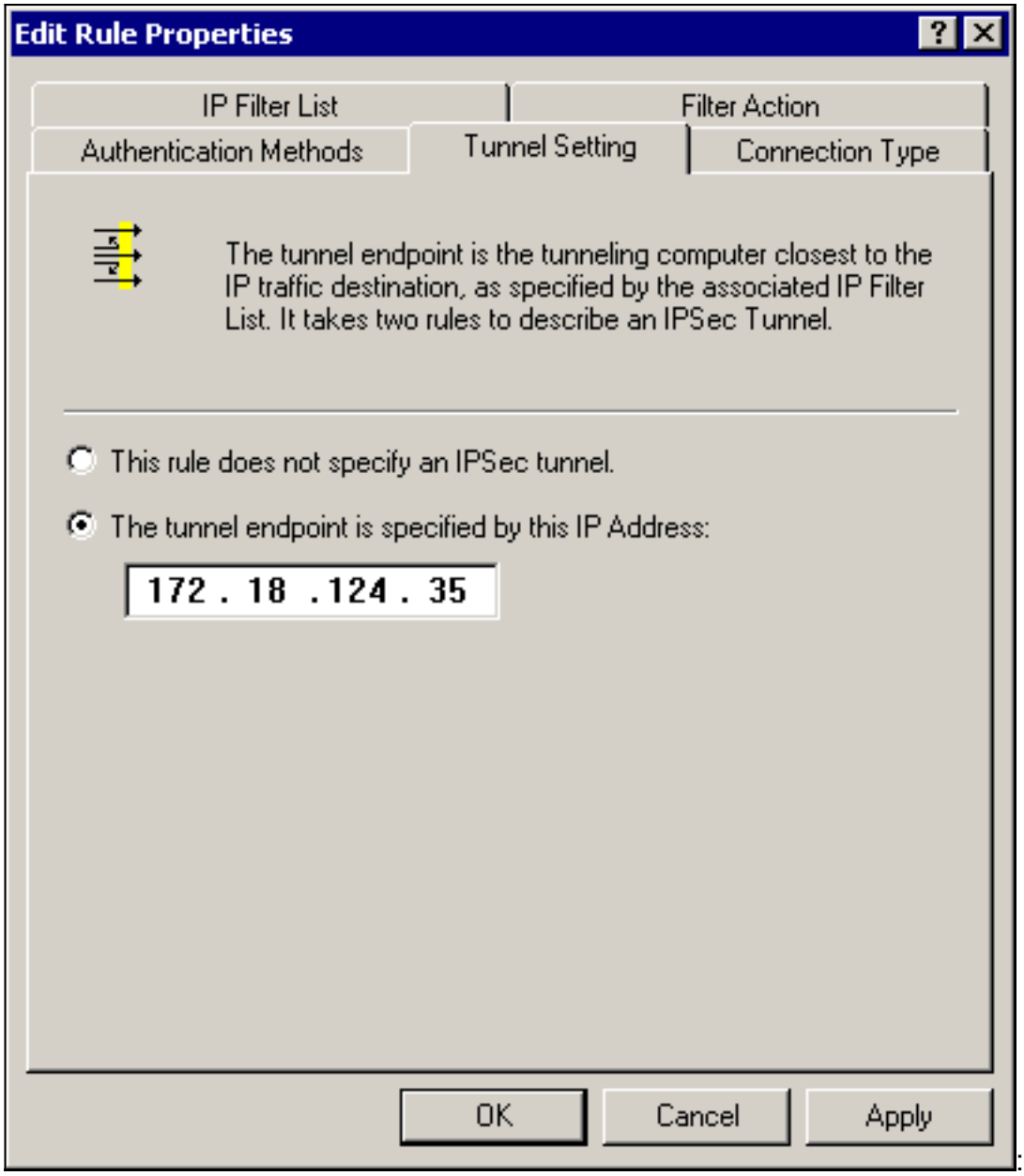
ل Microsoft-
Cisco:



إعداد النفق - نظائر التشفير:بالنسبة لشركة -Cisco



J:Microsoft



:Microsoft-Cisco

تكوين أجهزة Cisco

قم بتكوين موجهات Cisco و PIX و VPN Concentrator كما هو موضح في الأمثلة التالية.

- موجّه Cisco 3640
- PIX
- مركز VPN 3000
- مركز VPN 5000

تكوين الموجه Cisco 3640

موجّه Cisco 3640
Current configuration : 1840 bytes ! version 12.1 no service single-slot-reload-enable service timestamps debug uptime

```
service timestamps log uptime
no service password-encryption
!
hostname moss
!
logging rate-limit console 10 except errors
!
ip subnet-zero
!
no ip finger
!
ip audit notify log
ip audit po max-events 100
!
crypto isakmp policy 1
 The following are IOS defaults so they do not ---!
 appear: !--- IKE encryption method encryption des !---
 IKE hashing hash sha !--- Diffie-Hellman group group 1
 !--- Authentication method authentication pre-share
 IKE lifetime lifetime 28800 ---!
 encryption peer crypto isakmp key cisco123 address ---!
 172.18.124.157
!
 The following is the IOS default so it does not ---!
 appear: !--- IPSec lifetime crypto ipsec security-
 association lifetime seconds 3600 ! !--- IPSec
 transforms crypto ipsec transform-set rtpset esp-des
 esp-md5-hmac
!
crypto map rtp 1 ipsec-isakmp
 Encryption peer set peer 172.18.124.157 ---!
 set transform-set rtpset
 Source/Destination networks defined match address ---!
 115
!
call rsvp-sync
!
interface Ethernet0/0
ip address 192.168.1.1 255.255.255.0
ip nat inside
half-duplex
!
interface Ethernet0/1
ip address 172.18.124.35 255.255.255.240
ip nat outside
half-duplex
crypto map rtp
!
ip nat pool INTERNET 172.18.124.35 172.18.124.35 netmask
255.255.255.240
ip nat inside source route-map nonat pool INTERNET
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.124.36
no ip http server
!
access-list 101 deny ip 192.168.1.0 0.0.0.255 10.32.50.0
0.0.0.255
access-list 101 permit ip 192.168.1.0 0.0.0.255 any
 Source/Destination networks defined access-list 115 ---!
 permit ip 192.168.1.0 0.0.0.255 10.32.50.0 0.0.0.255
 access-list 115 deny ip 192.168.1.0 0.0.0.255 any
route-map nonat permit 10
match ip address 101
!
```

```
line con 0
transport input none
line 65 94
line aux 0
line vty 0 4
!
end
```

تهيئة PIX

PIX

```
(PIX Version 5.2(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 h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
Source/Destination networks defined access-list 115 ---!
permit ip 192.168.1.0 255.255.255.0 10.32.50.0
255.255.255.0
access-list 115 deny ip 192.168.1.0 255.255.255.0 any
pager lines 24
logging on
no logging timestamp
no logging standby
no logging console
no logging monitor
no logging buffered
no logging trap
no logging history
logging facility 20
logging queue 512
interface ethernet0 auto
interface ethernet1 10baset
mtu outside 1500
mtu inside 1500
ip address outside 172.18.124.35 255.255.255.240
ip address inside 192.168.1.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
arp timeout 14400
Except Source/Destination from Network Address ---!
Translation (NAT): nat (inside) 0 access-list 115
route outside 0.0.0.0 0.0.0.0 172.18.124.36 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
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
no sysopt route dnat
IPSec transforms crypto ipsec transform-set myset ---!
esp-des esp-md5-hmac
IPSec lifetime crypto ipsec security-association ---!
lifetime seconds 3600
crypto map rtpmap 10 ipsec-isakmp
Source/Destination networks crypto map rtpmap 10 ---!
match address 115
Encryption peer crypto map rtpmap 10 set peer ---!
172.18.124.157
crypto map rtpmap 10 set transform-set myset
crypto map rtpmap interface outside
isakmp enable outside
Encryption peer isakmp key ******** address ---!
172.18.124.157 netmask 255.255.255.240
isakmp identity address
Authentication method isakmp policy 10 ---!
authentication pre-share
IKE encryption method isakmp policy 10 encryption ---!
des
IKE hashing isakmp policy 10 hash sha ---!
Diffie-Hellman group isakmp policy 10 group 1 ---!
IKE lifetime isakmp policy 10 lifetime 28800 ---!
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:c237ed11307abea7b530bbd0c2b2ec08
end :
```

تكوين مركز VPN 3000

أستخدم خيارات القائمة والمعلمات الموضحة أدناه لتكوين مركز VPN حسب الحاجة.

- لإضافة مقترح IKE، حدد **التكوين > النظام > بروتوكولات الاتصال النفقي > IPSec > مقترحات IKE > إضافة مقترح.**

```
Proposal Name = DES-SHA
Authentication method Authentication Mode = Preshared Keys !--- IKE hashing ---!
Authentication Algorithm = SHA/HMAC-160 !--- IKE encryption method Encryption Algorithm =
DES-56 !--- Diffie-Hellman group Diffie Hellman Group = Group 1 (768-bits) Lifetime
Measurement = Time Date Lifetime = 10000 !--- IKE lifetime Time Lifetime = 28800
```

- لتحديد نفق من شبكة LAN إلى شبكة LAN، حدد **تكوين > نظام > بروتوكولات الاتصال النفقي > شبكة LAN إلى شبكة LAN ل IPSec.**

```
Name = to_2000
Interface = Ethernet 2 (Public) 172.18.124.35/28
Encryption peer Peer = 172.18.124.157 !--- Authentication method Digital Certs = none ---!
(Use Pre-shared Keys) Pre-shared key = cisco123 !--- IPSec transforms Authentication =
ESP/MD5/HMAC-128 Encryption = DES-56 !--- Use the IKE proposal IKE Proposal = DES-SHA
Autodiscovery = off !--- Source network defined Local Network Network List = Use IP
Address/Wildcard-mask below IP Address 192.168.1.0 Wildcard Mask = 0.0.0.255 !---
Destination network defined Remote Network Network List = Use IP Address/Wildcard-mask below
IP Address 10.32.50.0 Wildcard Mask 0.0.0.255
```

- لتعديل اقتران الأمان، حدد **تكوين > إدارة السياسة > إدارة حركة المرور > اقترانات الأمان > تعديل.**

```
SA Name = L2L-to_2000
Inheritance = From Rule
IPSec Parameters
IPSec transforms Authentication Algorithm = ESP/MD5/HMAC-128 Encryption Algorithm = ---!
DES-56 Encapsulation Mode = Tunnel PFS = Disabled Lifetime Measurement = Time Data Lifetime
= 10000 !--- IPSec lifetime Time Lifetime = 3600 Ike Parameters !--- Encryption peer IKE
Peer = 172.18.124.157 Negotiation Mode = Main !--- Authentication method Digital Certificate
= None (Use Preshared Keys) !--- Use the IKE proposal IKE Proposal DES-SHA
```

تكوين مركز VPN 5000

مركز VPN 5000

```
[ IP Ethernet 1:0 ]
Mode = Routed
SubnetMask = 255.255.255.240
IPAddress = 172.18.124.35

[ General ]
IPSecGateway = 172.18.124.36
"DeviceName = "cisco
EthernetAddress = 00:00:a5:f0:c8:00
DeviceType = VPN 5002/8 Concentrator
ConfiguredOn = Timeserver not configured
ConfiguredFrom = Command Line, from Console

[ IP Ethernet 0:0 ]
Mode = Routed
SubnetMask = 255.255.255.0
IPAddress = 192.168.1.1

[ Tunnel Partner VPN 1 ]
Encryption peer Partner = 172.18.124.157 !--- ---!
IPSec lifetime KeyLifeSecs = 3600 BindTo = "ethernet
1:0" !--- Authentication method SharedKey = "cisco123"
KeyManage = Auto !--- IPSec transforms Transform =
esp(md5,des) Mode = Main !--- Destination network
defined Peer = "10.32.50.0/24" !--- Source network
defined LocalAccess = "192.168.1.0/24" [ IP Static ]
10.32.50.0 255.255.255.0 VPN 1 1 [ IP VPN 1 ] Mode =
Routed Numbered = Off [ IKE Policy ] !--- IKE hashing,
encryption, Diffie-Hellman group Protection = SHA_DES_G1
.Configuration size is 1088 out of 65500 bytes
```

التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك إستخدامها لاستكشاف أخطاء التكوينات وإصلاحها.

أوامر استكشاف الأخطاء وإصلاحها

يتم دعم بعض أوامر **العرض بواسطة** أداة مترجم الإخراج (العملاء المسجلون فقط)، والتي تتيح لك عرض تحليل

إخراج أمر **العرض**.

ملاحظة: قبل إصدار أوامر **تصحيح الأخطاء**، يرجى الاطلاع على المعلومات المهمة في أوامر تصحيح الأخطاء.

موجّه Cisco 3640

- **debug crypto Engine** - يعرض رسائل تصحيح الأخطاء حول محركات التشفير، التي تنفذ التشفير وفك التشفير.
- **debug crypto isakmp** - يعرض رسائل حول أحداث IKE.
- **debug crypto ipSec** - يعرض أحداث IPSec.
- **show crypto isakmp sa** - يعرض جميع اقترانات أمان IKE الحالية (SAs) في نظير.
- **show crypto ipSec** - يعرض الإعدادات المستخدمة من قبل اقترانات الأمان الحالية.
- **مسح التشفير isakmp** - (من وضع التكوين) مسح جميع إتصالات IKE النشطة.
- **مسح crypto sa** - (من وضع التكوين) يحذف جميع اقترانات أمان IPSec.

PIX

- **debug crypto ipSec** - يعرض مفاوضات IPSec للمرحلة 2.
- **debug crypto isakmp** - يعرض مفاوضات بروتوكول إدارة المفاتيح وارتباط أمان الإنترنت (ISAKMP) للمرحلة 1.
- **debug crypto Engine** - يعرض حركة مرور البيانات التي يتم تشفيرها.
- **show crypto ips sa** - يعرض اقترانات أمان المرحلة 2.
- **show crypto isakmp sa** - يعرض اقترانات أمان المرحلة 1.
- **مسح تشفير isakmp** - (من وضع التكوين) مسح اقترانات أمان تبادل مفتاح الإنترنت (IKE).
- **مسح** اقترانات أمان IPSec **للتشفير** IPsec - (من وضع التكوين).

مركز VPN 3000

- - بدء تصحيح أخطاء مركز VPN 3000 من خلال تحديد **التكوين > النظام > الأحداث > الفئات > تعديل** (الخطورة إلى السجل=1-13، الخطورة إلى وحدة التحكم=1-3): IKE، IKEDBG، IKEdecode، IPSec، IPSECDBG، IPSECDECODE
- - يمكن مسح سجل الأحداث أو إسترداده من خلال تحديد **مراقبة > سجل الأحداث**.
- - ال lan إلى lan نفق حركة مرور يستطيع كنت monitore في **monitore>جلسة**.
- - يمكن مسح النفق في **الإدارة > جلسات الإدارة > جلسات عمل شبكة LAN إلى شبكة LAN > إجراءات - تسجيل الخروج.**

مركز VPN 5000

- **VPN Trace Dump all** - يعرض معلومات حول جميع إتصالات VPN المطابقة، بما في ذلك معلومات حول الوقت، ورقم شبكة VPN، وعنوان IP الحقيقي للنظير، الذي تم تشغيل البرامج النصية، وفي حالة حدوث خطأ، الروتين ورقم سطر رمز البرنامج حيث حدث الخطأ.
- **show vpn statistics** - يعرض المعلومات التالية للمستخدمين والشركاء والإجمالي لكل من. (للطرز النمطية، يتضمن العرض قسما لكل فتحة وحدة نمطية.) Active الحالي - الاتصالات النشطة الحالية. في المفاوضات - الاتصالات التفاوضية الحالية. High Water - أعلى عدد من الاتصالات النشطة المتزامنة منذ آخر إعادة تشغيل. إجمالي التشغيل - إجمالي عدد الاتصالات الناجحة منذ آخر عملية إعادة تشغيل. بدء النفق - عدد بدء النفق. Tunnel OK - عدد الأنفاق التي لا توجد أخطاء فيها. خطأ نفق - عدد الأنفاق التي تحتوي على أخطاء.
- **show vpn statistics verbose** - يعرض إحصائيات تفاوض ISAKMP، وإحصاءات اتصال أكثر نشاطا.

معلومات ذات صلة

- إعلان نهاية المبيعات لسلسلة Cisco VPN 5000
- تكوين أمان شبكة IPSec
- تكوين بروتوكول أمان Internet Key Exchange
- الدعم الفني - 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).