# تكوين نفق IPSec - مركز VPN 3000 من Cisco إلى جدار حماية رقم 4.1

## المحتويات



## المقدمة

يوضح هذا المستند كيفية تكوين نفق IPsec بمفاتيح مشتركة مسبقا للانضمام إلى شبكتين خاصتين:

- شبكة خاصة داخل مركز Cisco VPN 3000 (192.168.1.x).
- شبكة خاصة داخل جدار حماية نقطة التفتيش 4.1 (x.10.32.50).

يفترض أن حركة المرور من داخل مركز الشبكة الخاصة الظاهرية (VPN) وداخل نقطة التفتيش إلى الإنترنت (ممثلة في هذا المستند بشبكات x.172.18.124) تتدفق قبل أن يبدأ هذا التكوين.

## المتطلبات الأساسية

### المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

### المكونات المستخدمة

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

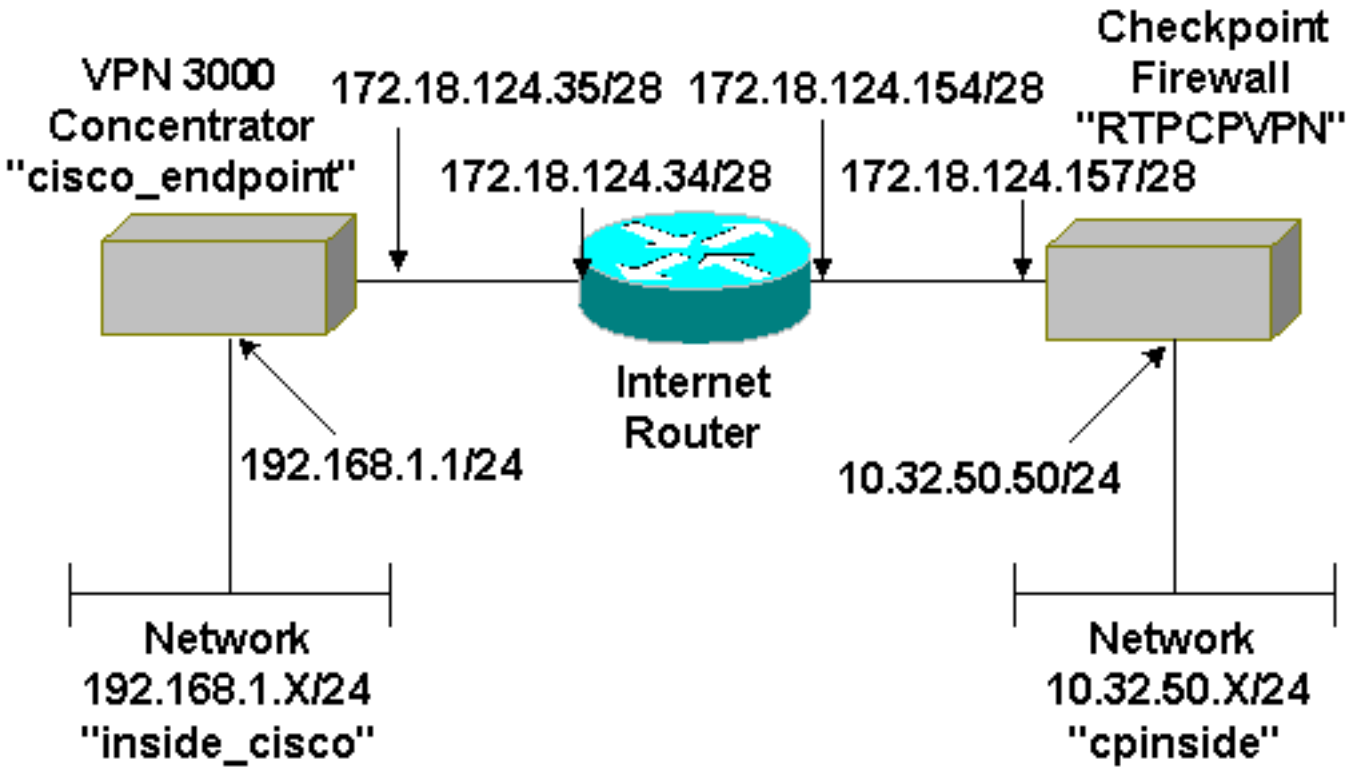
- مركز VPN 3000

- برنامج مركز VPN 3000، الإصدار F.2.5.2
- جدار حماية نقطة التفتيش 4.1

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.

## الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



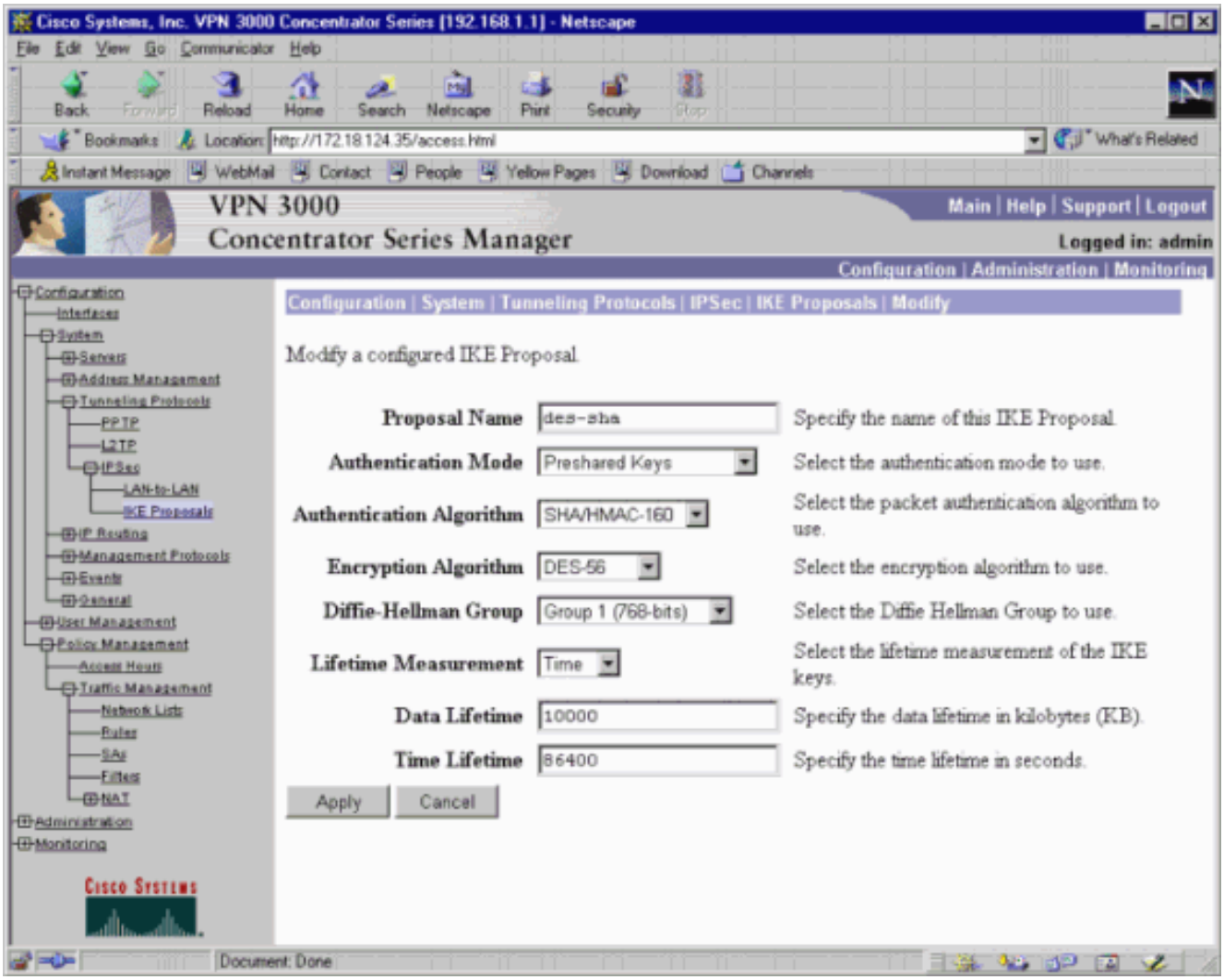

## الاصطلاحات

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

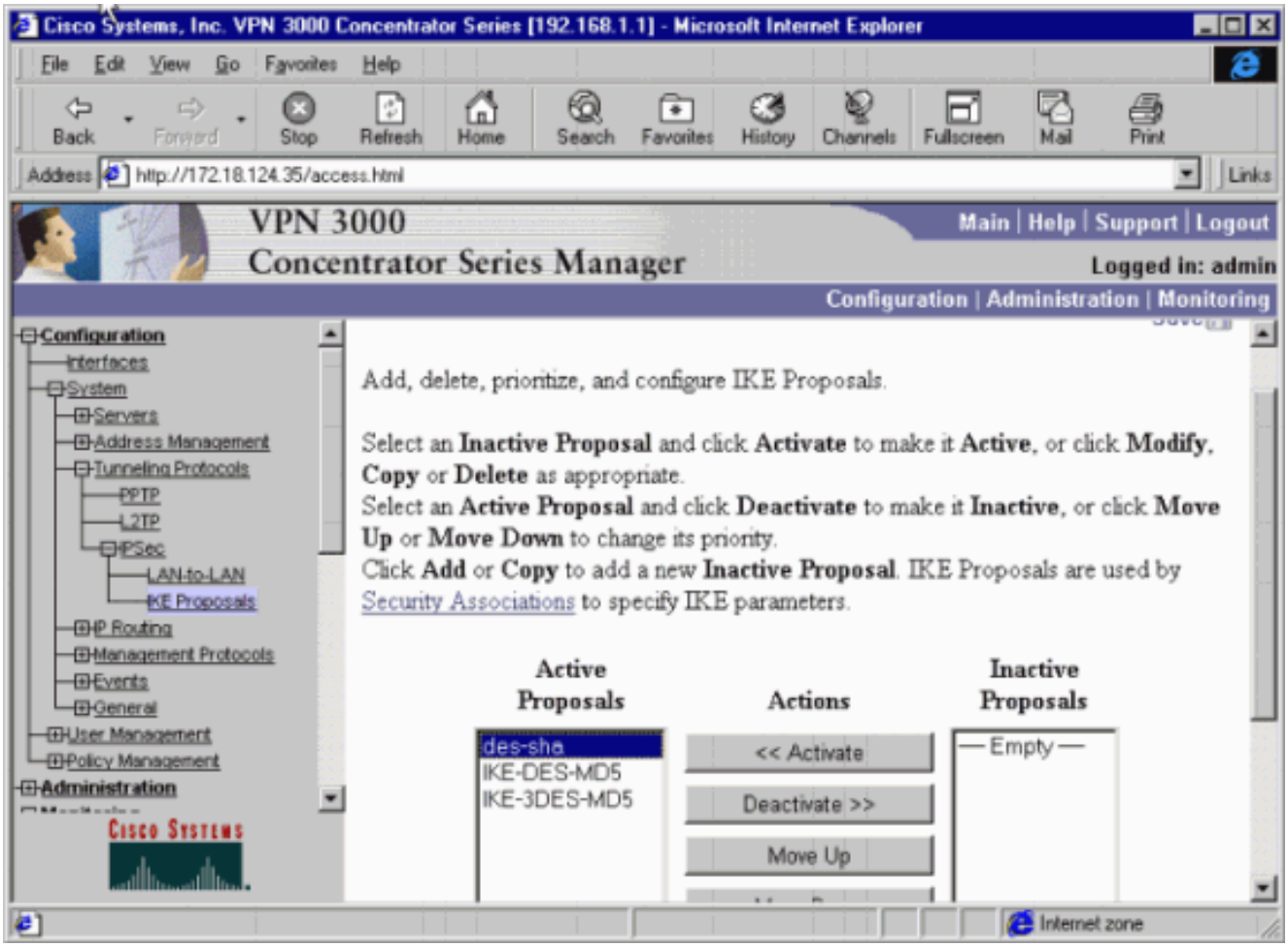
# تكوين مركز VPN 3000

أكمل هذه الخطوات لتكوين مركز VPN 3000.

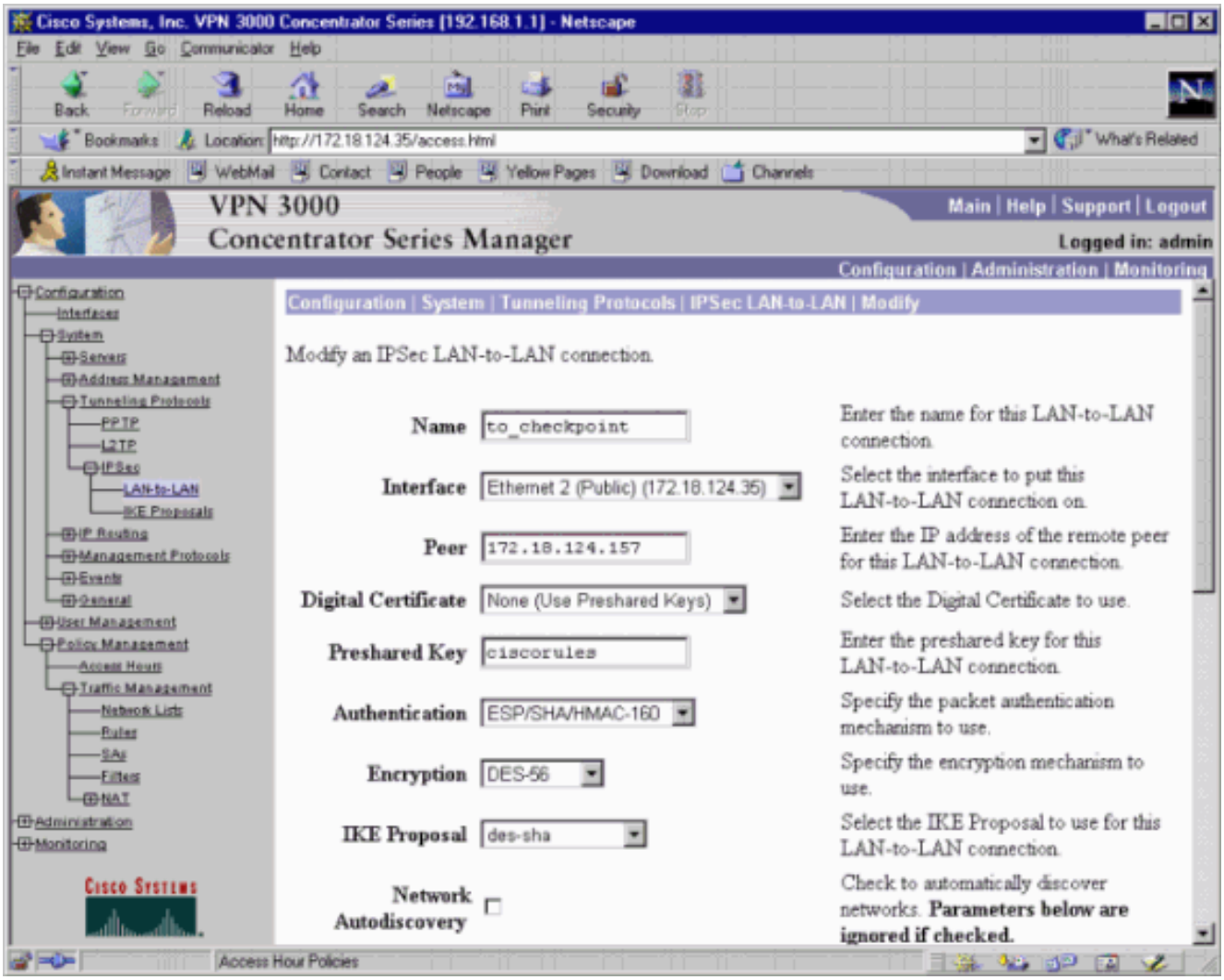
1. حدد **تكوين > نظام > بروتوكولات الاتصال النفقي > IPSec > مقترحات IKE > تعديل** لإنشاء اقتراح تبادل مفتاح إنترنت (IKE) باسم "des-sha" مع تجزئة خوارزمية التجزئة الآمنة (SHA) ومعيار تشفير البيانات (DES) ومجموعة Diffie-hellman 1. أترك العمر الافتراضي للوقت في 86400 ثانية.**ملاحظة:** يبلغ النطاق الصحيح لفترة وجود IKE لمكثف VPN من 60 إلى 2147483647 ثانية.

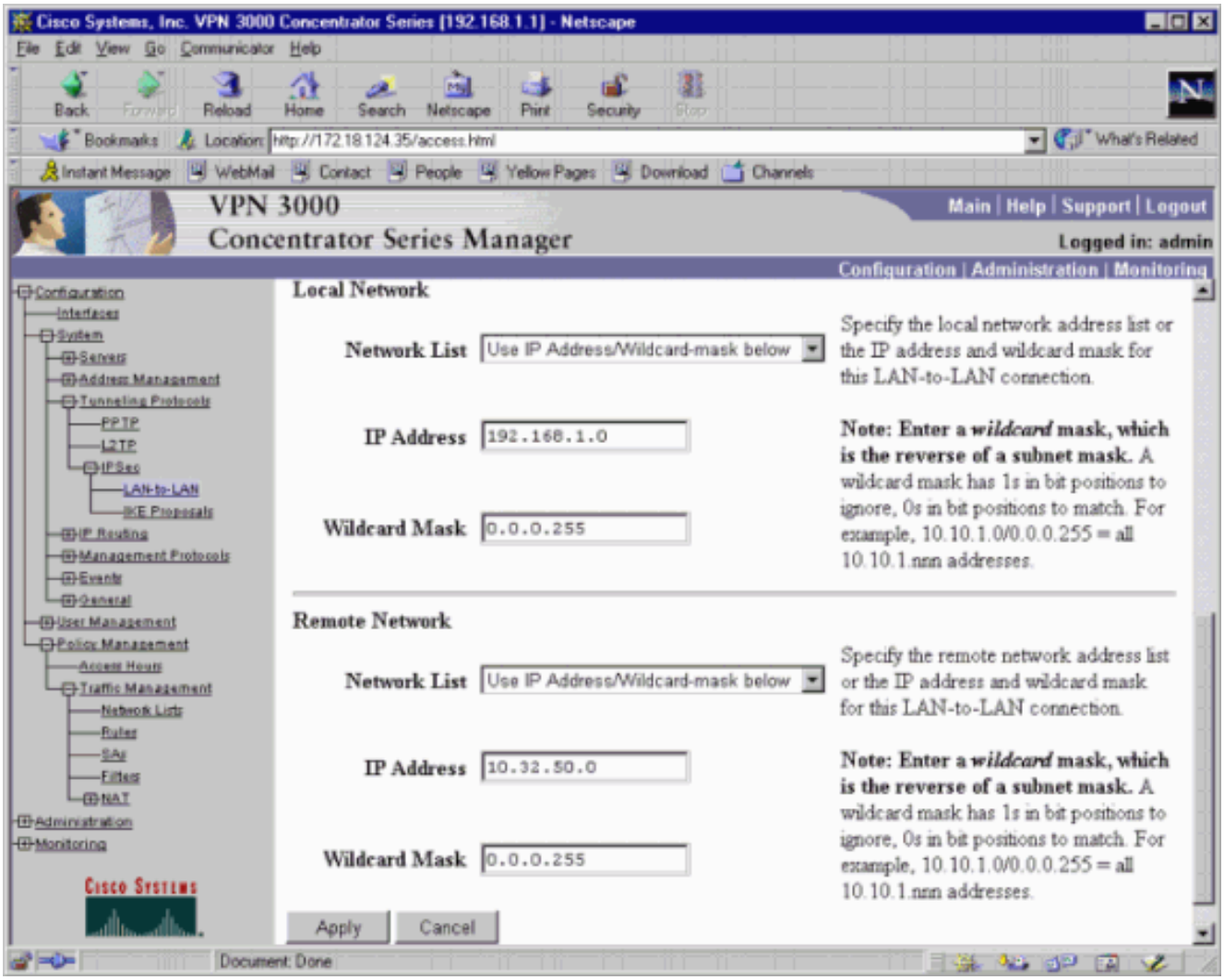



2. حدد **تكوين > نظام > بروتوكولات الاتصال النفقي > IPSec > مقترحات IKE**. حدد "des-sha" وانقر فوق **تنشيط** لتنشيط اقتراح IKE.

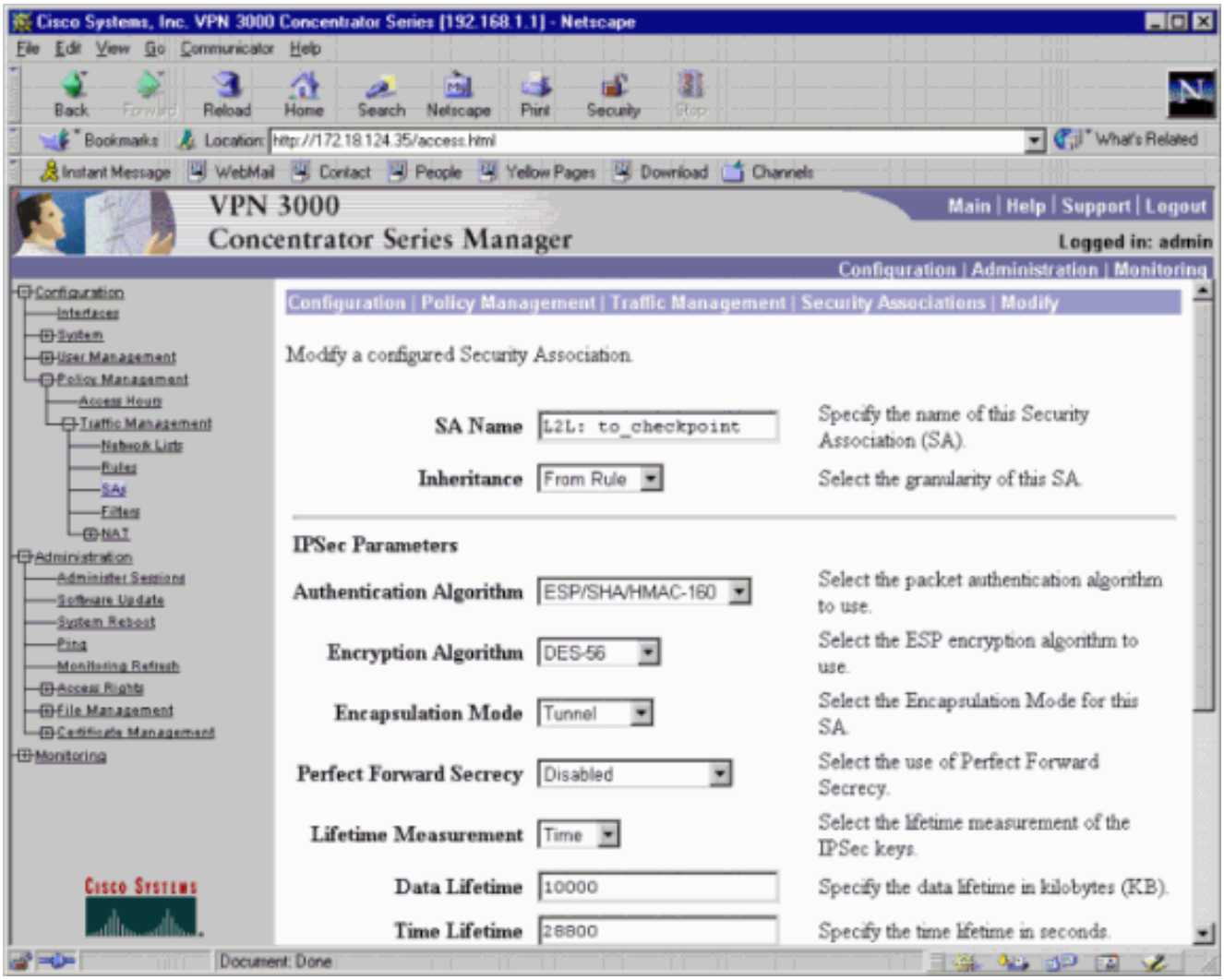


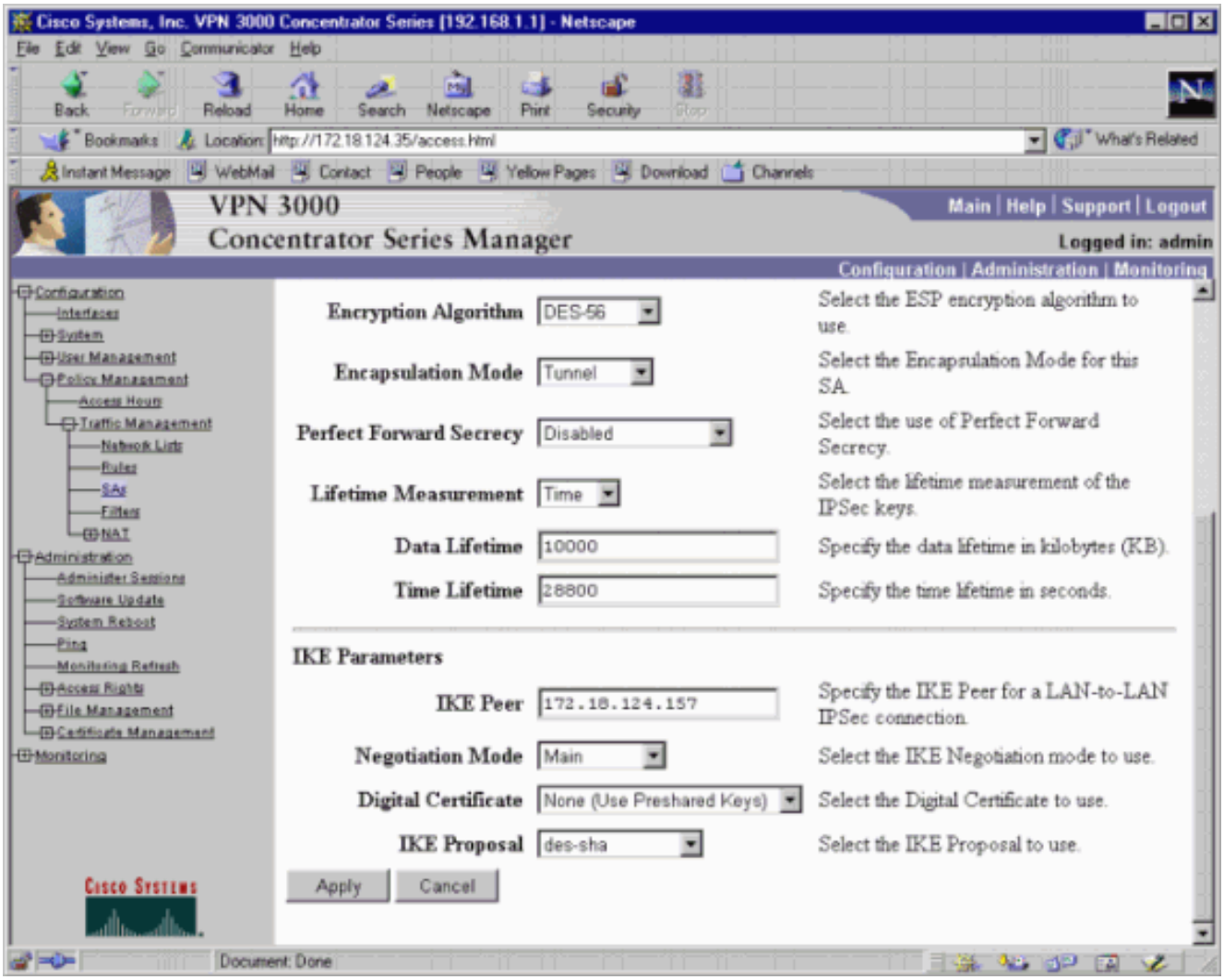

3. حدد **تكوين > نظام > بروتوكولات الاتصال النفقي > IPSec LAN إلى شبكة LAN > إضافة**.قم بإعداد نفق IPsec يسمى "to_checkpoint" باستخدام عنوان نقطة التفتيش كالنظير. بالنسبة للمفتاح المشترك مسبقا، أدخل المفتاح الفعلي. تحت المصادقة، حدد ESP/SHA/HMAC-160، وحدد DES-56 للتشفير. أدخل اقتراح IKE ("des-sha" في هذا المثال)، والشبكات المحلية والبعيدة.


Cisco Systems, Inc. VPN 3000 Concentrator Series [192.168.1.1] - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: http://172.18.124.35/access.html
What's Related
Instant Message WebMail Contact People Yellow Pages Download Channels
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
Servers
Address Management
Tunneling Protocols
PPTP
L2TP
IPSec
LAN-to-LAN
IKE Proposals
IP Routing
Management Protocols
Events
General
User Management
Policy Management
Access Hours
Traffic Management
Network Lists
Rules
SAs
Filters
NAT
Administration
Monitoring
Cisco Systems
Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Modify
Modify an IPSec LAN-to-LAN connection.
Name
to_checkpoint
Enter the name for this LAN-to-LAN connection.
Interface
Ethernet 2 (Public) (172.18.124.35)
Select the interface to put this LAN-to-LAN connection on.
Peer
172.18.124.157
Enter the IP address of the remote peer for this LAN-to-LAN connection.
Digital Certificate
None (Use Preshared Keys)
Select the Digital Certificate to use.
Preshared Key
ciscorules
Enter the preshared key for this LAN-to-LAN connection.
Authentication
ESP/SHA/HMAC-160
Specify the packet authentication mechanism to use.
Encryption
DES-56
Specify the encryption mechanism to use.
IKE Proposal
des-sha
Select the IKE Proposal to use for this LAN-to-LAN connection.
Network Autodiscovery
Check to automatically discover networks. Parameters below are ignored if checked.
Access Hour Policies




4. حدد **تشكيل > إدارة السياسة > إدارة حركة المرور > اقترانات التأمين > تعديل**. تحقق من **تعطيل** سرية إعادة التوجيه المثالية وترك العمر الزمني ل IPsec في **الثواني** الافتراضية **28800**.**ملاحظة:** يبلغ النطاق الصحيح لفترة وجود IPsec لمركز تركيز الشبكة الخاصة الظاهرية (VPN) من 60 إلى 2147483647 ثانية.


Cisco Systems, Inc. VPN 3000 Concentrator Series [192.168.1.1] - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: http://172.18.124.35/access.html What's Related
Instant Message WebMail Contact People Yellow Pages Download Channels
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Access Hours
Traffic Management
Network Lists
Rules
SAs
Filters
NAT
Administration
Administer Sessions
Software Update
System Reboot
Ping
Monitoring Refresh
Access Rights
File Management
Certificate Management
Monitoring
Configuration | Policy Management | Traffic Management | Security Associations | Modify
Modify a configured Security Association.
SA Name
L2L: to_checkpoint
Specify the name of this Security Association (SA).
Inheritance
From Rule
Select the granularity of this SA.
IPSec Parameters
Authentication Algorithm
ESP/SHA/HMAC-160
Select the packet authentication algorithm to use.
Encryption Algorithm
DES-56
Select the ESP encryption algorithm to use.
Encapsulation Mode
Tunnel
Select the Encapsulation Mode for this SA.
Perfect Forward Secrecy
Disabled
Select the use of Perfect Forward Secrecy.
Lifetime Measurement
Time
Select the lifetime measurement of the IPSec keys.
Data Lifetime
10000
Specify the data lifetime in kilobytes (KB).
Time Lifetime
28800
Specify the time lifetime in seconds.
Cisco Systems
Document: Done

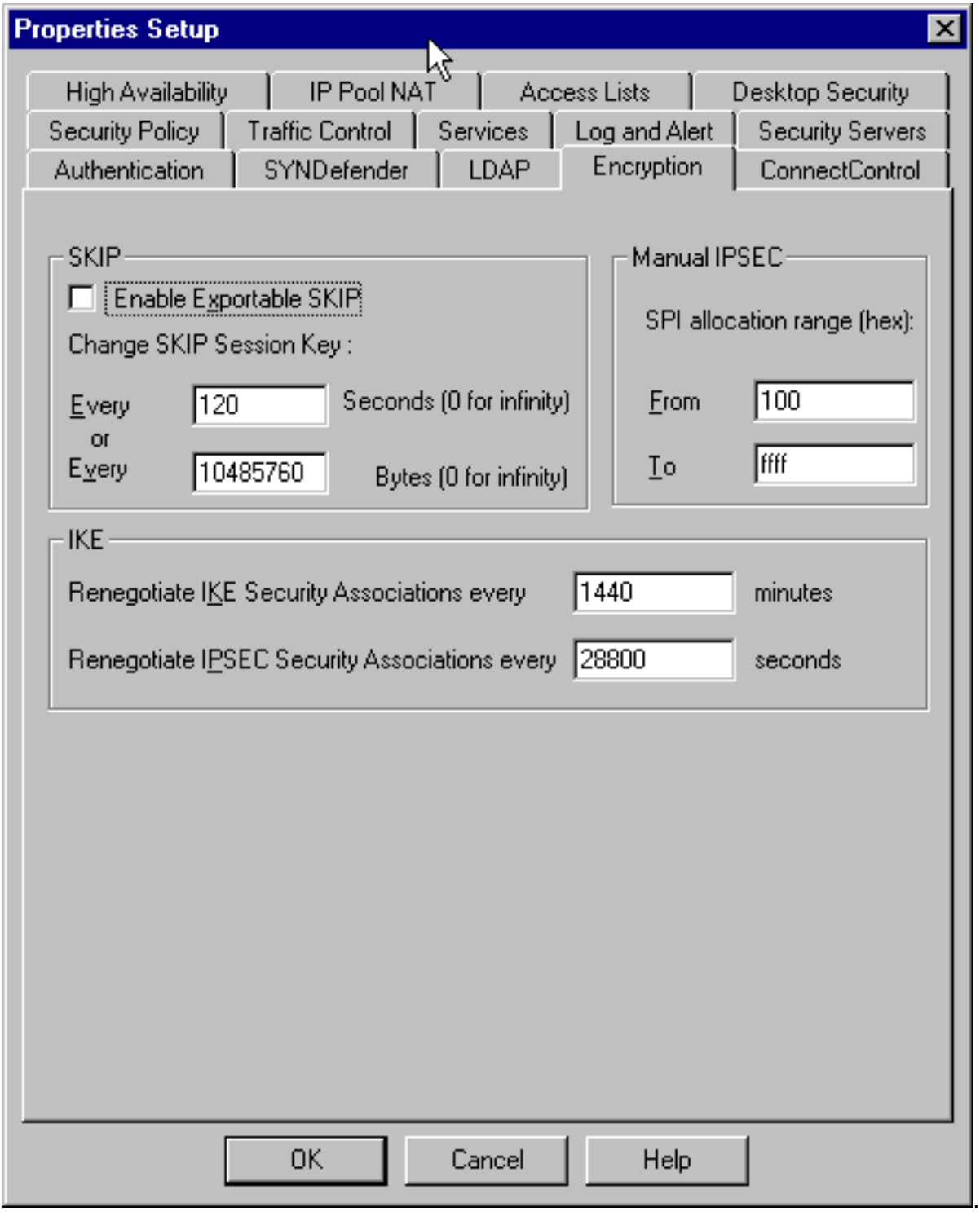



5. قم بحفظ التكوين.

## تكوين جدار حماية نقطة الوصول 4.1

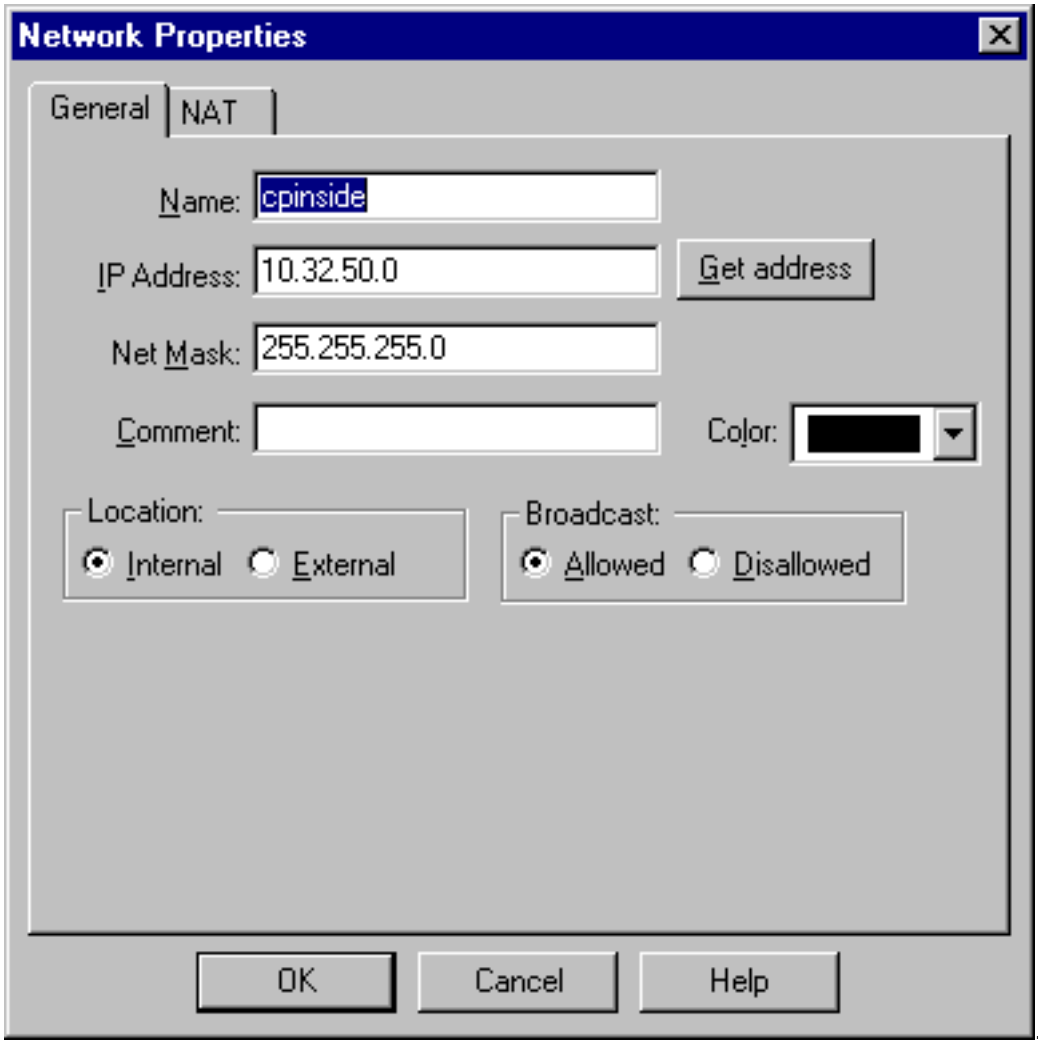
أكمل الخطوات التالية لتكوين جدار حماية نقطة الوصول 4.1.

1. ونظرا لاختلاف مدد الحياة الافتراضية لبروتوكول IKE و IPsec بين الموردين، حدد **خصائص > تشفير** لتعيين فترات حياة نقطة الوصول للاتفاق مع إعدادات مركز الشبكة الخاصة الظاهرية (VPN) الافتراضية.مدة بقاء IKE الافتراضية لمحرك الشبكة الخاصة الظاهرية (VPN) هي 86400 ثانية (=1440 دقيقة).مدة بقاء مركز VPN الافتراضي ل IPsec هي 28800



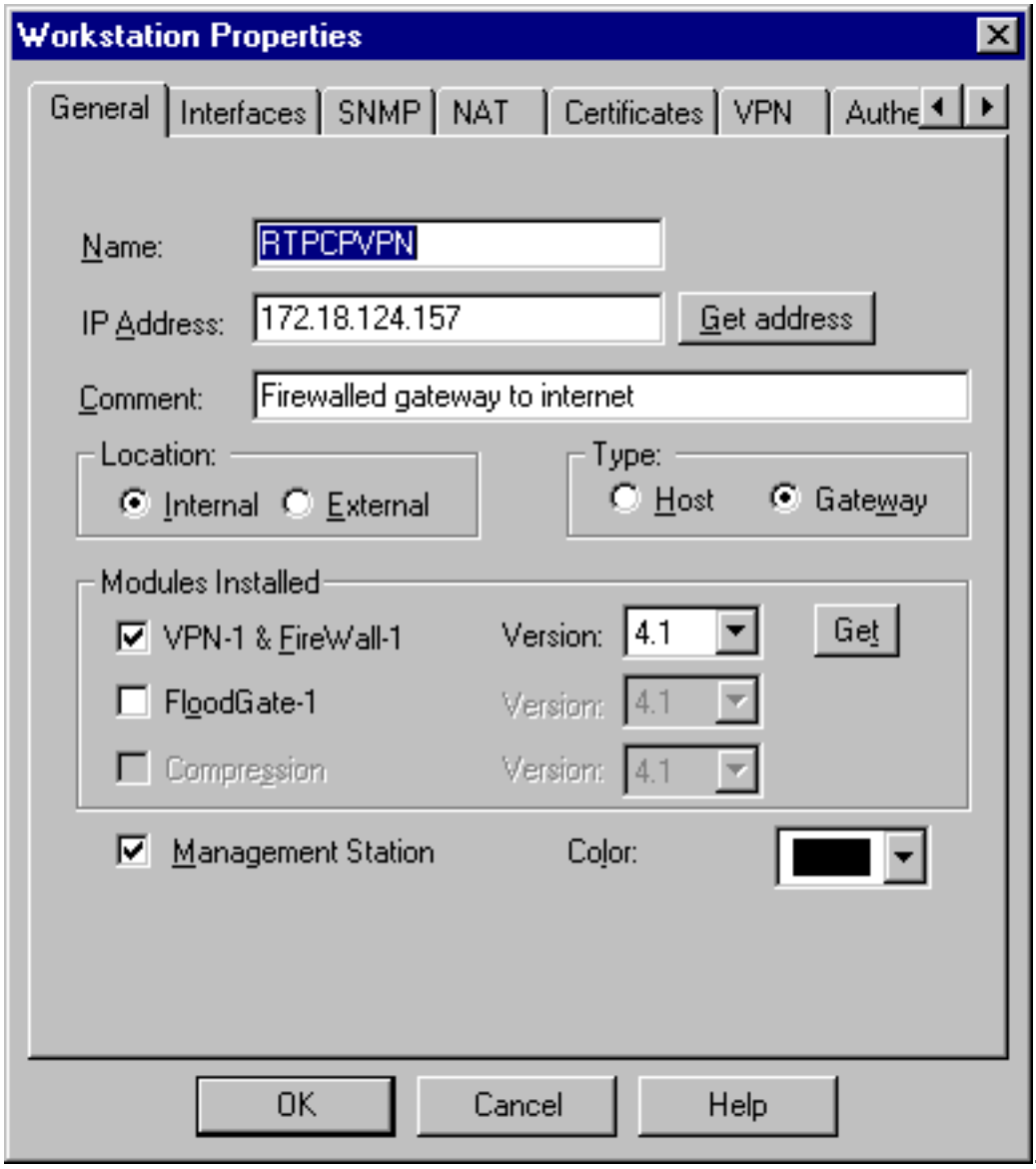

ثانية.

2. حدد **إدارة > كائنات الشبكة > جديد (أو تحرير) > الشبكة** لتكوين الكائن للشبكة الداخلية ("CPINSIDE") خلف نقطة التفتيش. يجب أن يتوافق ذلك مع "الشبكة البعيدة" في مركز الشبكة الخاصة الظاهرية



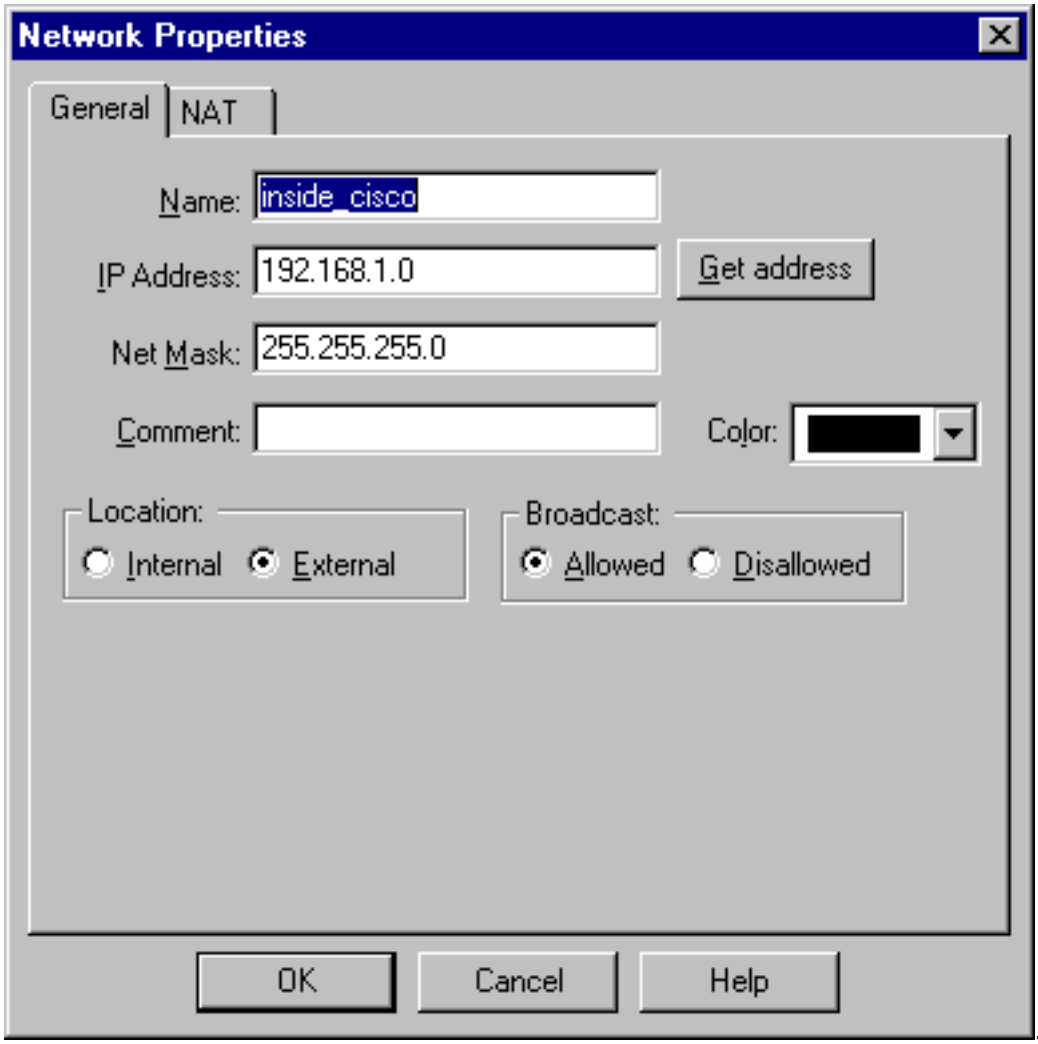

(VPN).

3. حدد **إدارة > كائنات الشبكة > تحرير** لتحرير الكائن لنقطة النهاية للبوابة ("نقطة تفتيش RTPCPVPN") التي يمتلكها مركز VPN في معلمة النظير.تحت الموقع، حدد **داخلي**. للنوع، حدد **البوابة**. تحت الوحدات المثبتة، تحقق من **VPN-1 و FireWall-1** وافحص **محطة**



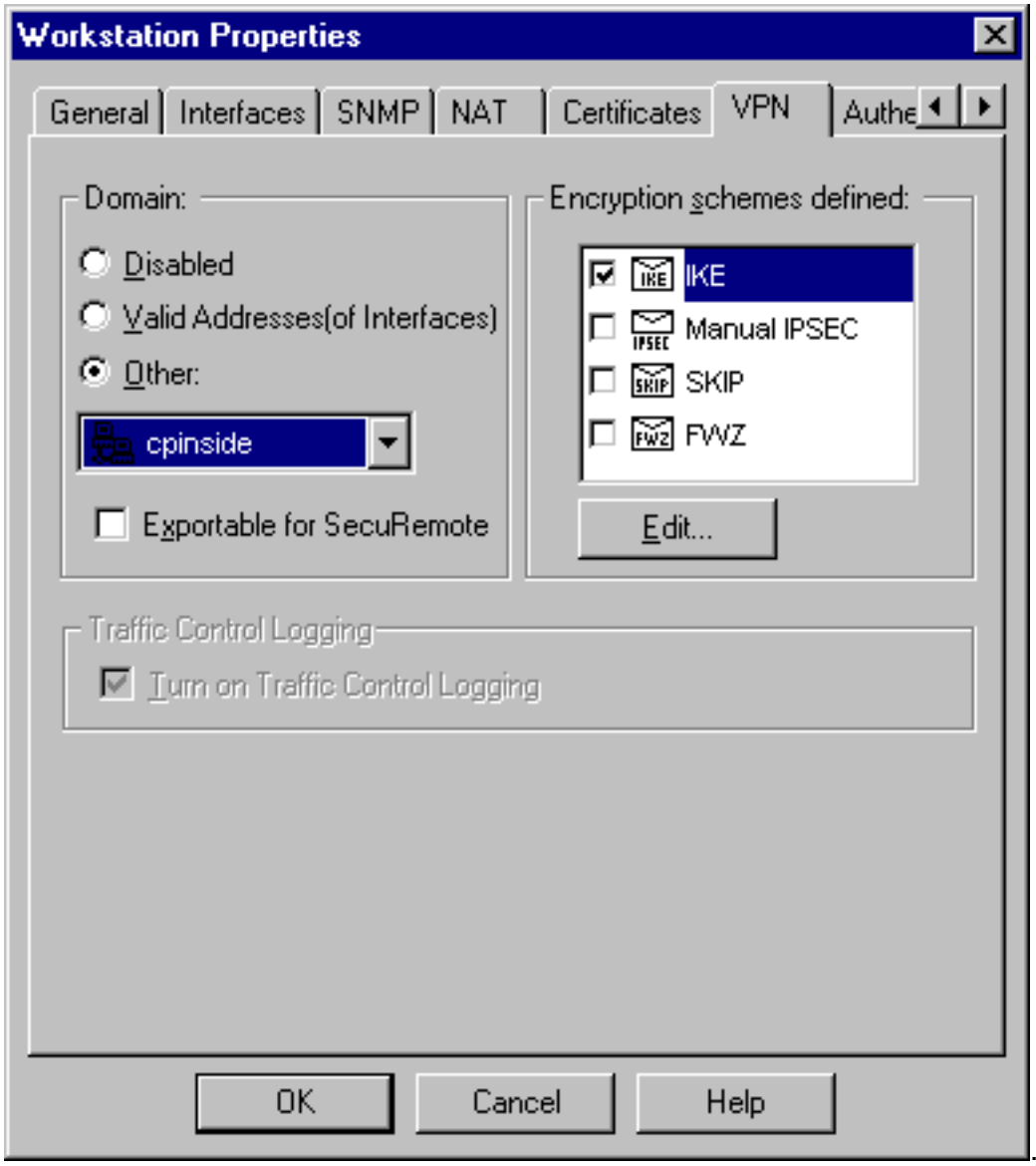

**الإدارة**.

4. حدد **إدارة > كائنات الشبكة > جديد (أو تحرير) > الشبكة** لتكوين الكائن للشبكة الخارجية ("inside_cisco") خلف مركز VPN. يجب أن يتوافق ذلك مع الشبكة "المحلية" في مركز الشبكة الخاصة الظاهرية



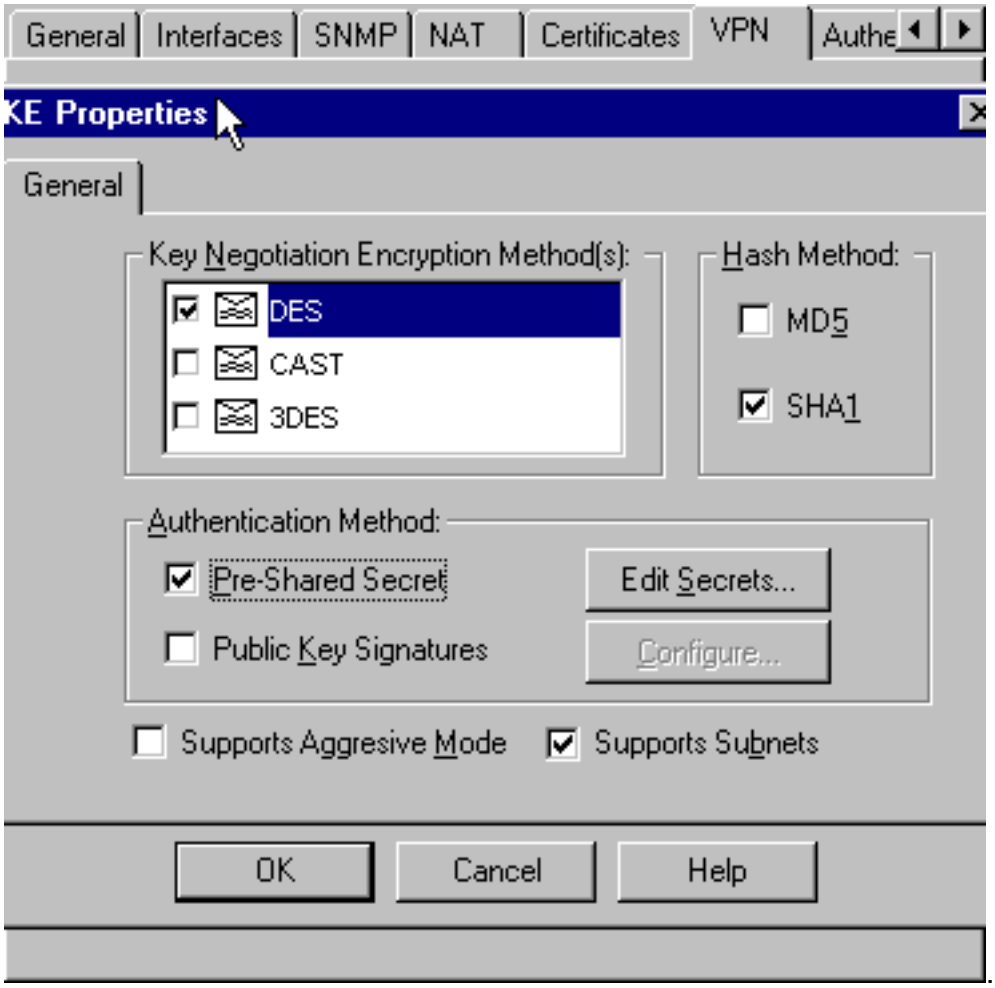

(VPN).

5. حدد **إدارة > كائنات الشبكة > جديد > محطة عمل** لإضافة كائن لبوابة مركز VPN الخارجية ("Cisco_Endpoint"). هذه هي واجهة مركز الشبكة الخاصة الظاهرية (VPN) "العامة".تحت الموقع، حدد **خارجي**. للنوع، حدد **البوابة.ملاحظة:** لا تحدد خانة الاختيار VPN-1/FireWall-1.
6. حدد **إدارة > كائنات الشبكة > تحرير** لتحرير نقطة نهاية عبارة نقطة النهاية (تسمى "RTPCPVPN") لعلامة التبويب VPN. تحت المجال، حدد "آخر" ثم حدد داخل شبكة نقطة التفتيش (والتي تسمى "cpinside") من القائمة المنسدلة. تحت تشفير نظام يعين، حدد **IKE**، ثم انقر



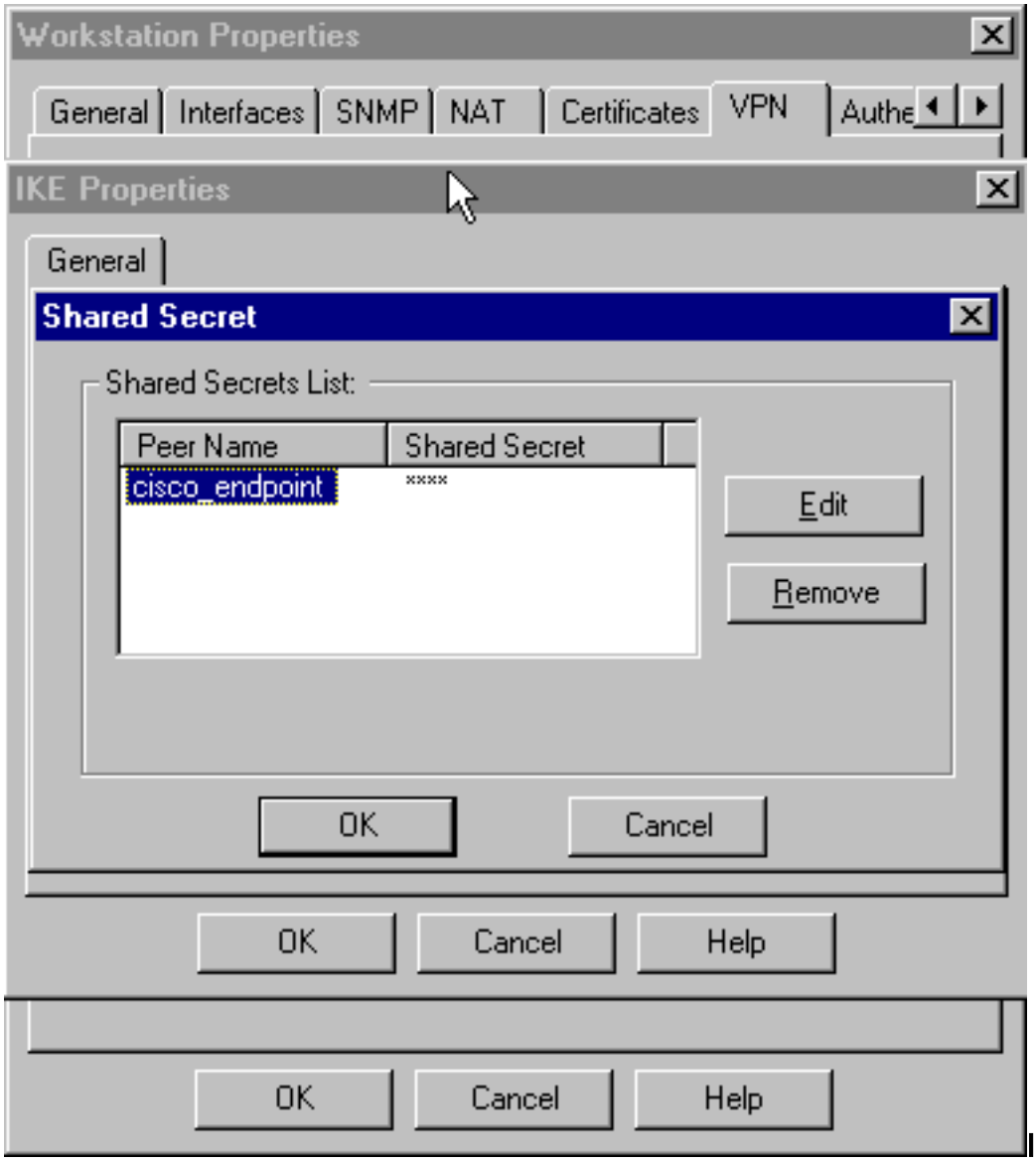

**تحرير**.

7. قم بتغيير خصائص IKE لتشفير DES لتتوافق مع **DES-56** وخوارزمية **التشفير** على مركز VPN.
8. قم بتغيير خصائص IKE إلى تجزئة SHA1 للاتفاق مع خوارزمية 160-**SHA/HMAC** في مركز VPN.عدم تحديد **الوضع المتداخل**.تحقق من **دعم الشبكات الفرعية**.تحقق من **سر مشترك مسبقا** تحت أسلوب المصادقة. وهذا يتوافق مع وضع مصادقة مركز الشبكة الخاصة الظاهرية (VPN)، والمفاتيح المحددة



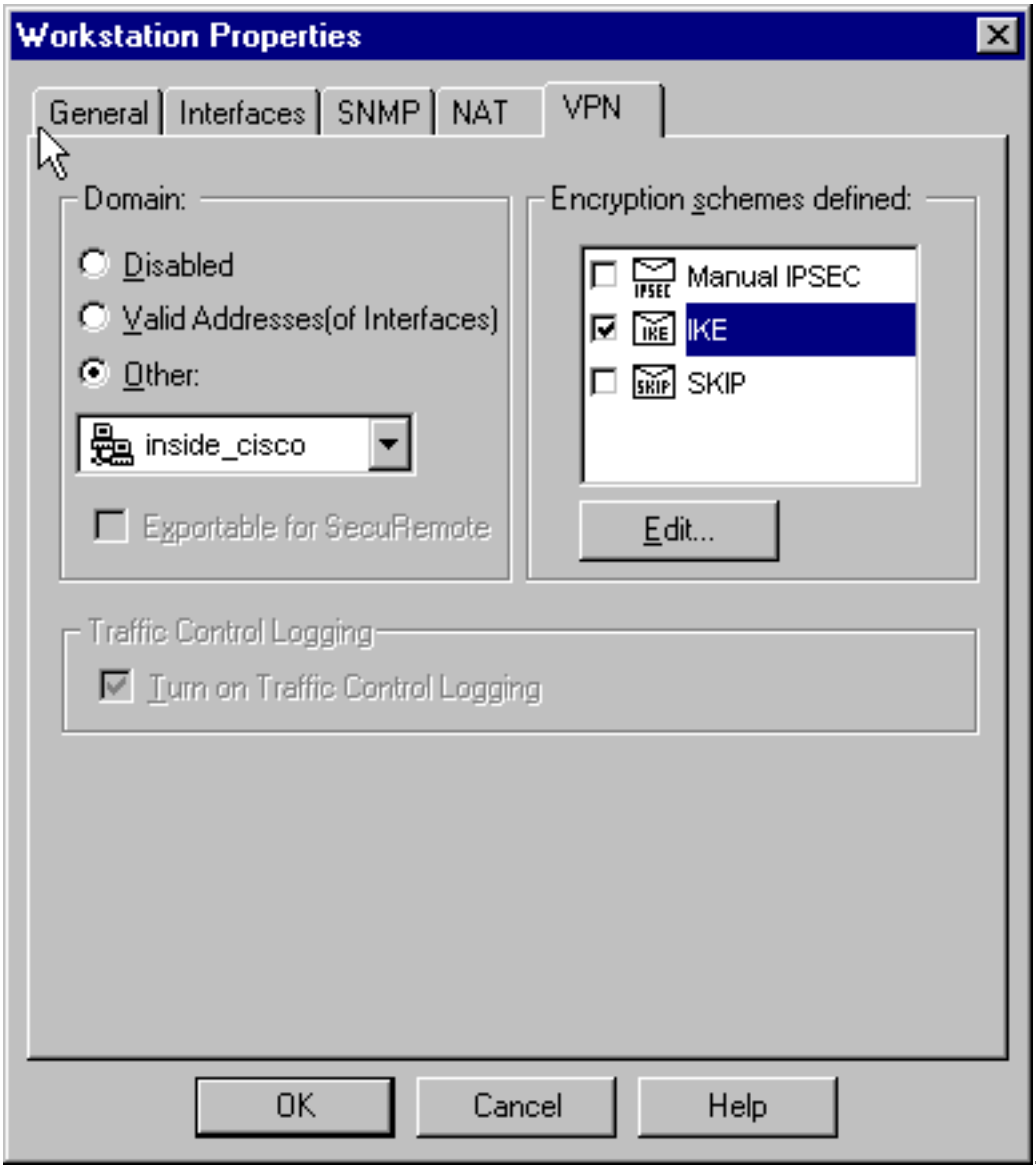
مسبقا.

9. انقر فوق **تحرير الأسرار** لتعيين المفتاح المشترك مسبقا للموافقة على **المفتاح** المحدد مسبقا الخاص بمجمع VPN الفعلي.**قناع الشبكة الخاص بعنوان قناع الشبكة (NETMASK) الخاص بعنوان مفتاح**



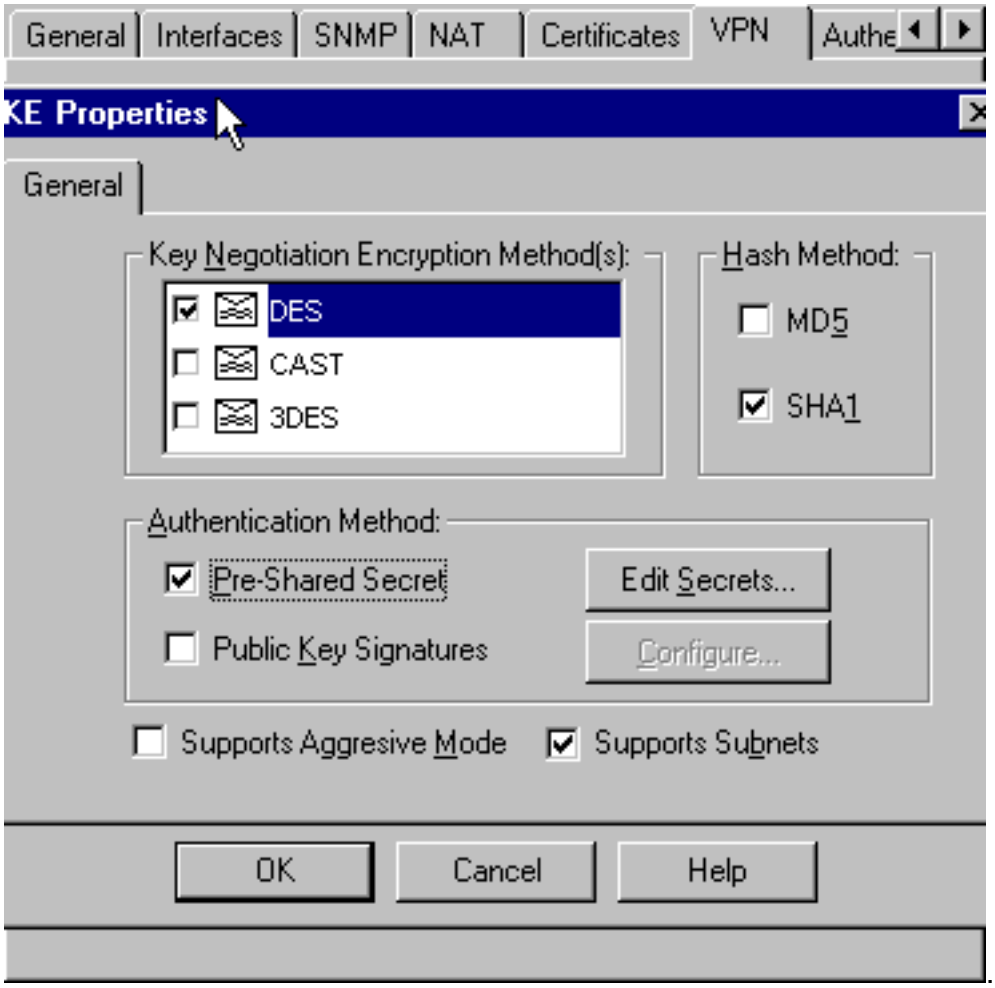

ISAKMP

10. حدد **إدارة > كائنات الشبكة > تحرير** لتحرير علامة التبويب cisco_endpoint" VPN". تحت مجال، حدد **آخر**، ثم حدد داخل شبكة Cisco (تسمى "inside_cisco"). تحت تشفير نظام يعين، حدد **IKE**، ثم انقر



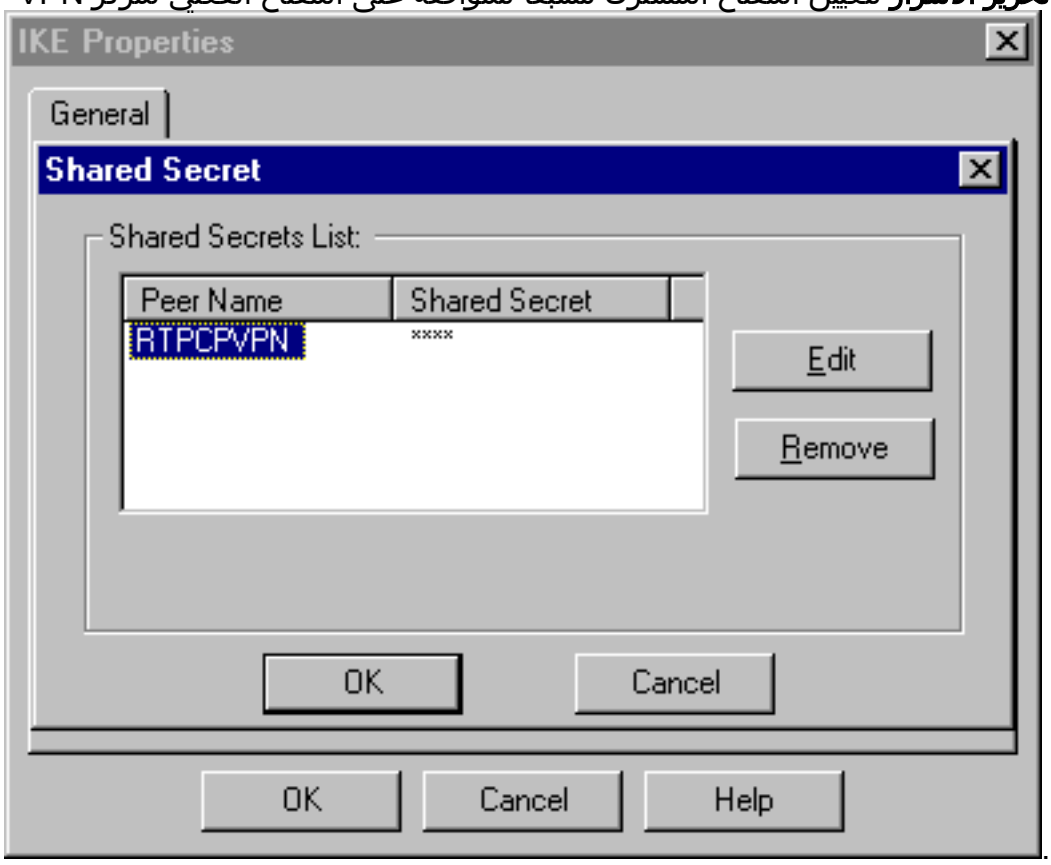

**تحرير**.

11. قم بتغيير تشفير خصائص IKE DES للاتفاق مع **خوارزمية التشفير DES-56** على مركز VPN.
12. قم بتغيير خصائص IKE إلى تجزئة SHA1 للاتفاق مع خوارزمية 160-**SHA/HMAC** في مركز VPN.تغيير هذه الإعدادات:**حالة إلغاء التحديد**.تحقق من **دعم الشبكات الفرعية**.تحقق من **سر مشترك مسبقا** تحت أسلوب المصادقة. وهذا يتوافق مع وضع مصادقة مركز الشبكة الخاصة الظاهرية (VPN) للمفاتيح المحددة




مسبقا.

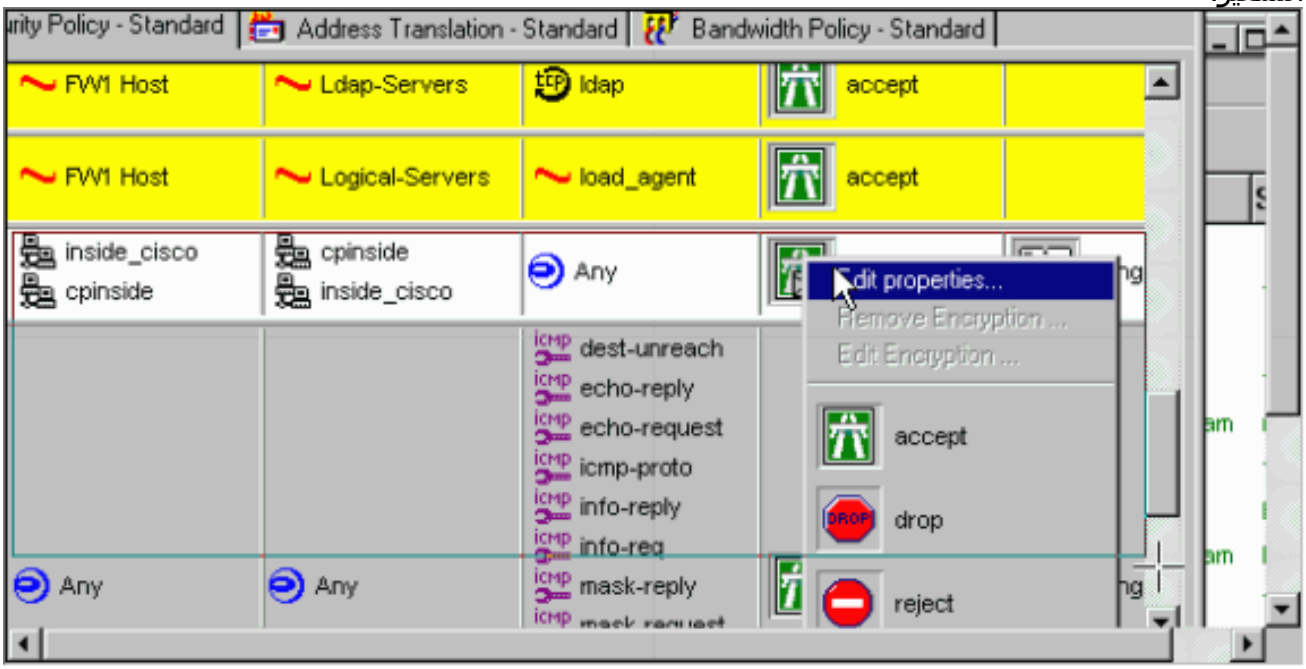
13. انقر فوق **تحرير الأسرار** لتعيين المفتاح المشترك مسبقا للموافقة على المفتاح الفعلي لمركز VPN



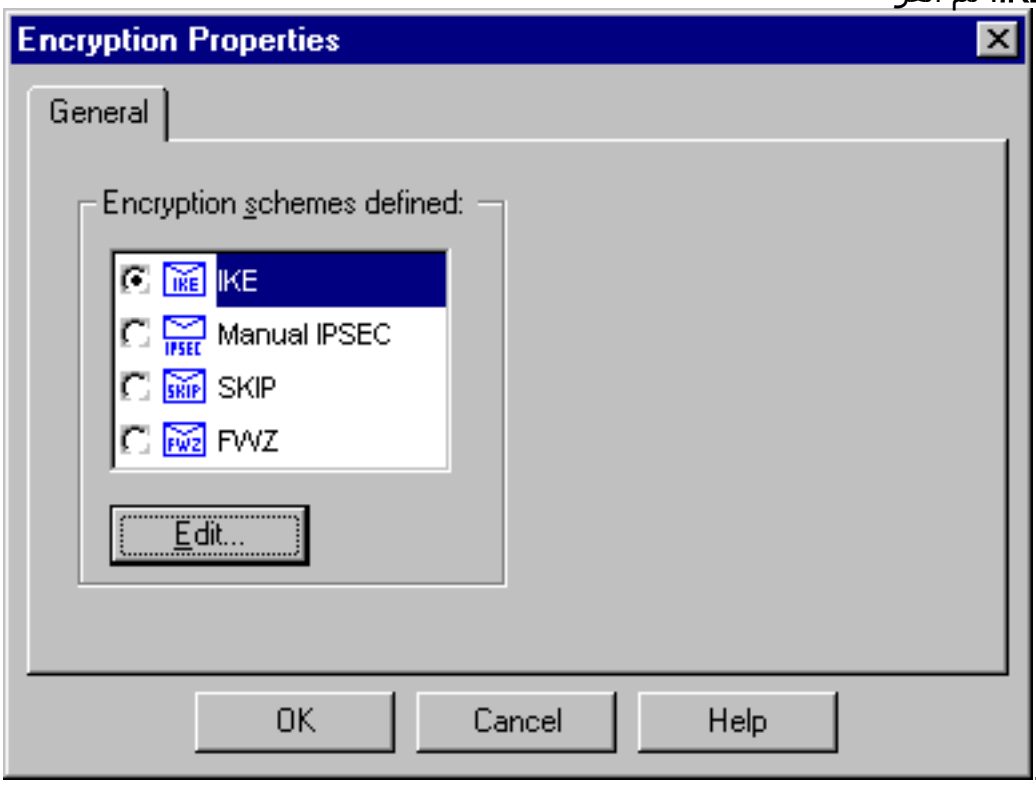

المضغوط.

14. في نافذة "محرر النهج"، قم بإدراج قاعدة بكل من "المصدر والوجهة" و"inside_cisco" و"cpinside" (ثنائي الإتجاه). تعيين الخدمة=أي، الإجراء=التشفير، والتتبع=طويل.


15. تحت عنوان الإجراء، انقر على أيقونة **التشفير** الأخضر وحدد **تحرير الخصائص** لتكوين سياسات التشفير.

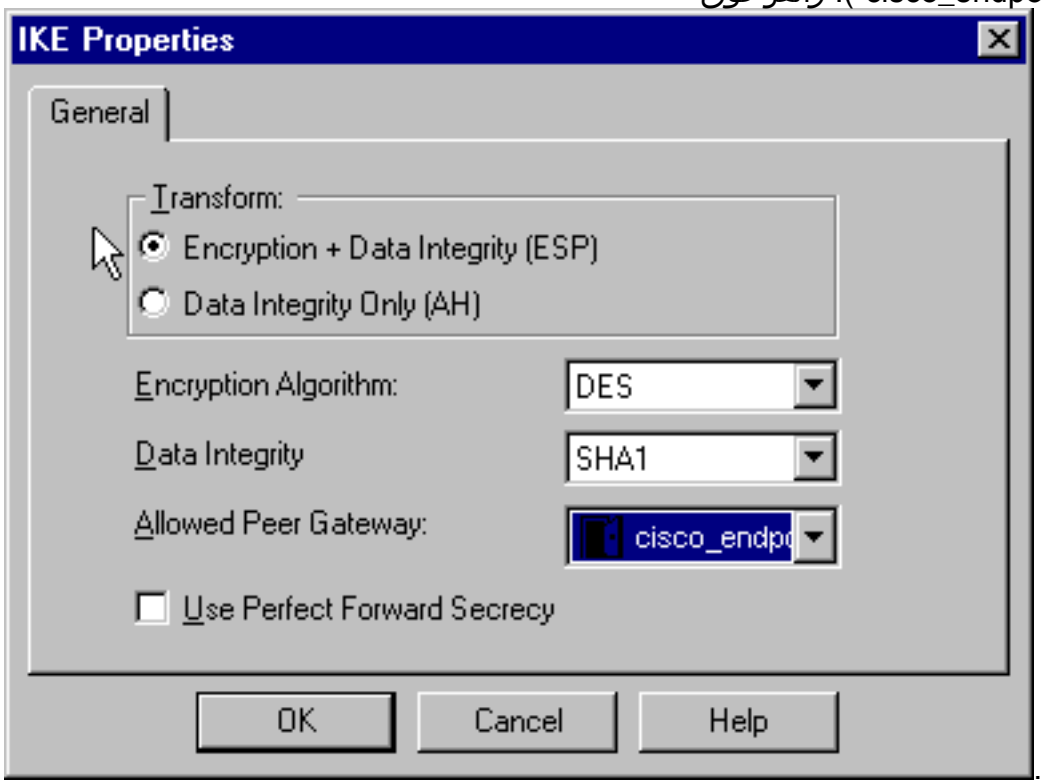



16. حدد **IKE**، ثم انقر




**تحرير**.

17. في نافذة خصائص IKE، قم بتغيير هذه الخصائص لتوافق مع عمليات تحويل IPsec لحوامل تركيز VPN.تحت التحويل، حدد **التشفير + تكامل البيانات (ESP)**. يجب أن تكون خوارزمية التشفير **DES**، ويجب أن تكون سلامة البيانات SHA1، ويجب أن تكون بوابة النظير المسموح بها عبارة Cisco الخارجية (التي تسمى "cisco_endpoint"). وانقر فوق




.OK

18. بعد تكوين نقطة التحقق، حدد **نهج > تثبيت** في قائمة نقطة التفتيش لتفعيل التغييرات.

## التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

## استكشاف الأخطاء وإصلاحها

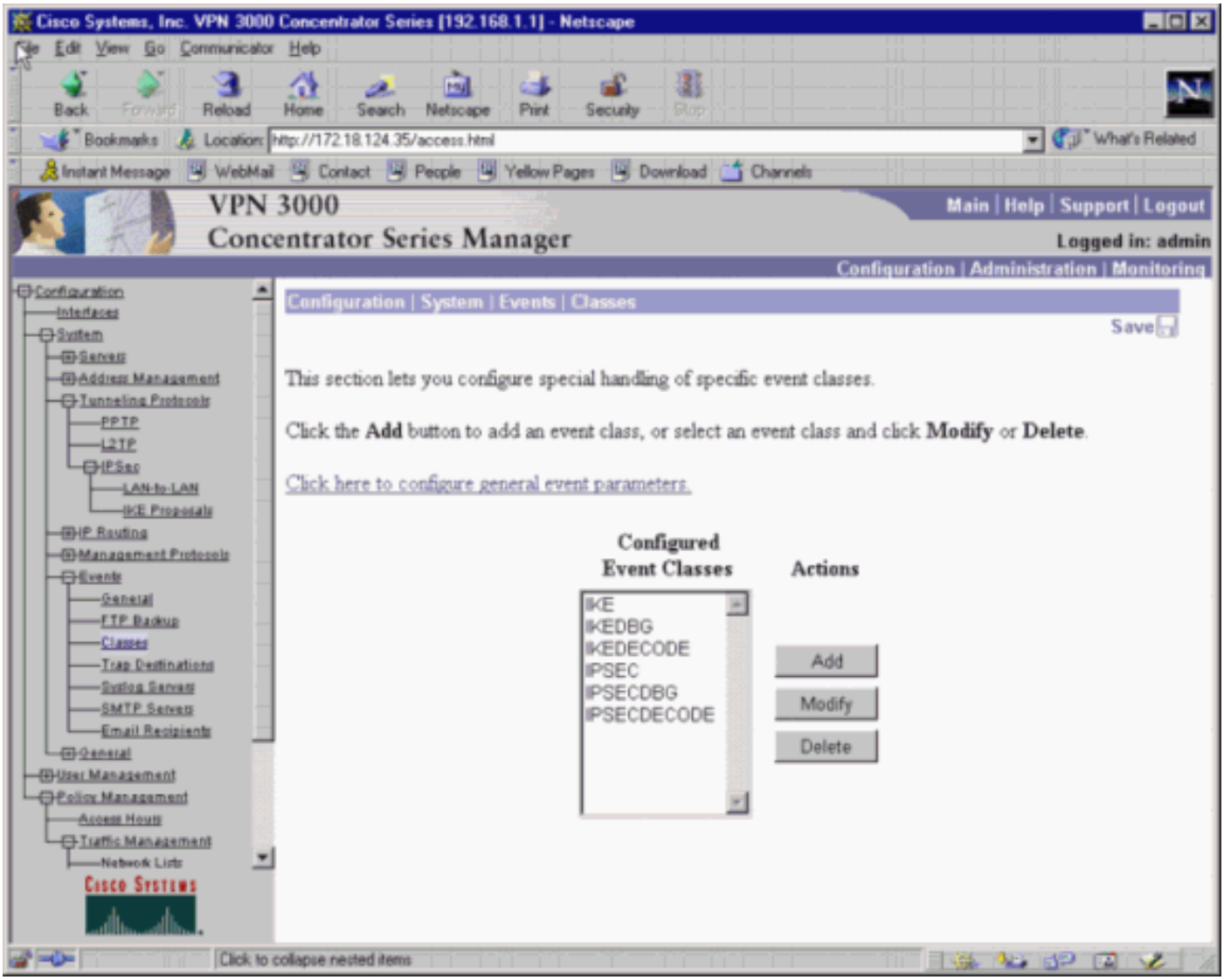
يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

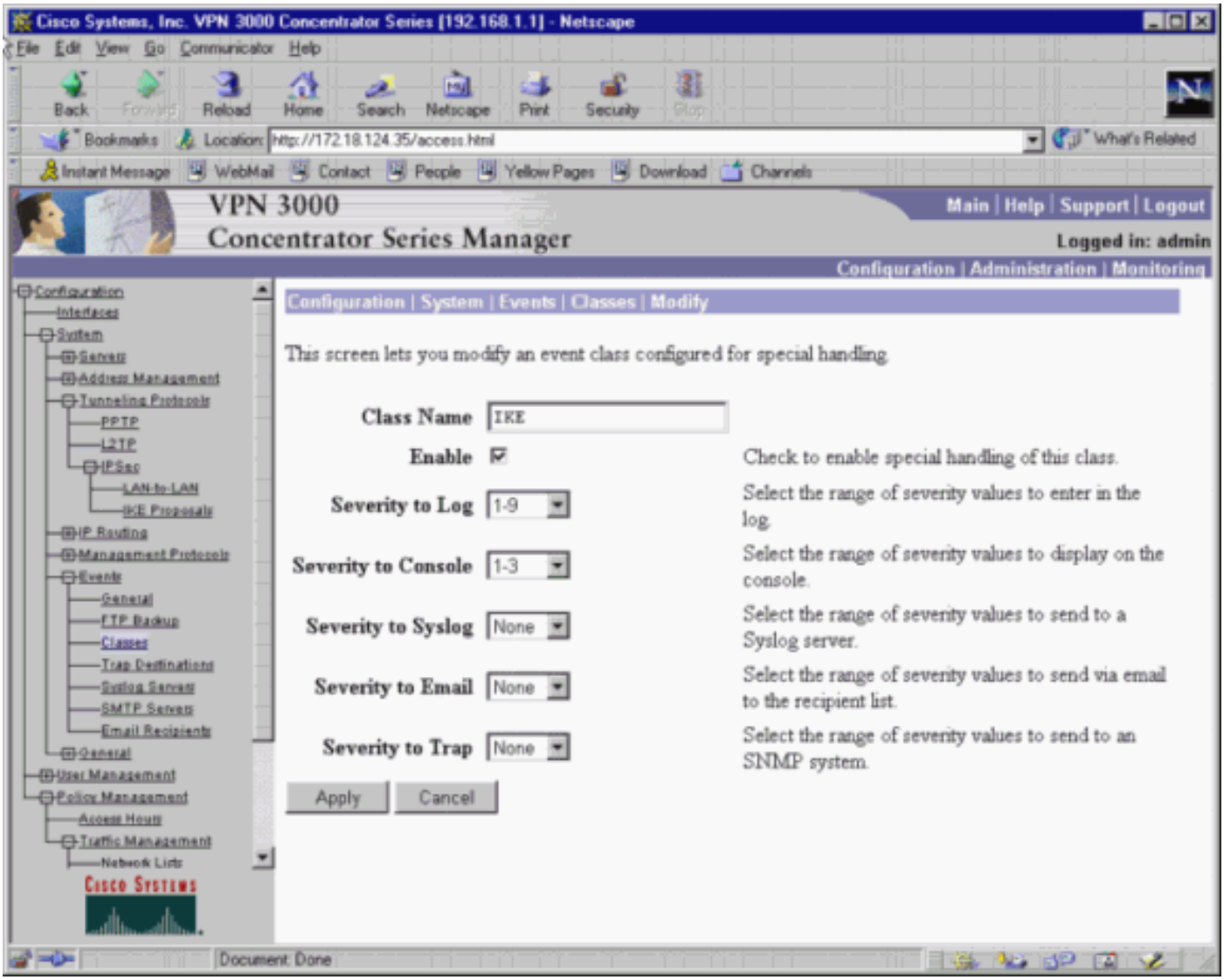
### تلخيص الشبكة

عندما يتم تكوين شبكات داخلية متجاورة متعددة في مجال التشفير على نقطة التحقق، قد يقوم الجهاز بتلخيصها تلقائيا فيما يتعلق بحركة المرور المفيدة. إذا لم يتم تكوين مركز الشبكة الخاصة الظاهرية (VPN) ليتطابق، فمن المحتمل أن يفشل النفق. على سبيل المثال، إذا تم تكوين الشبكات الداخلية من 10.0.0.0 /24 و 10.0.1.0 /24 لتضمينها في النفق، فقد يتم تلخيصها إلى 10.0.0.0 /23.

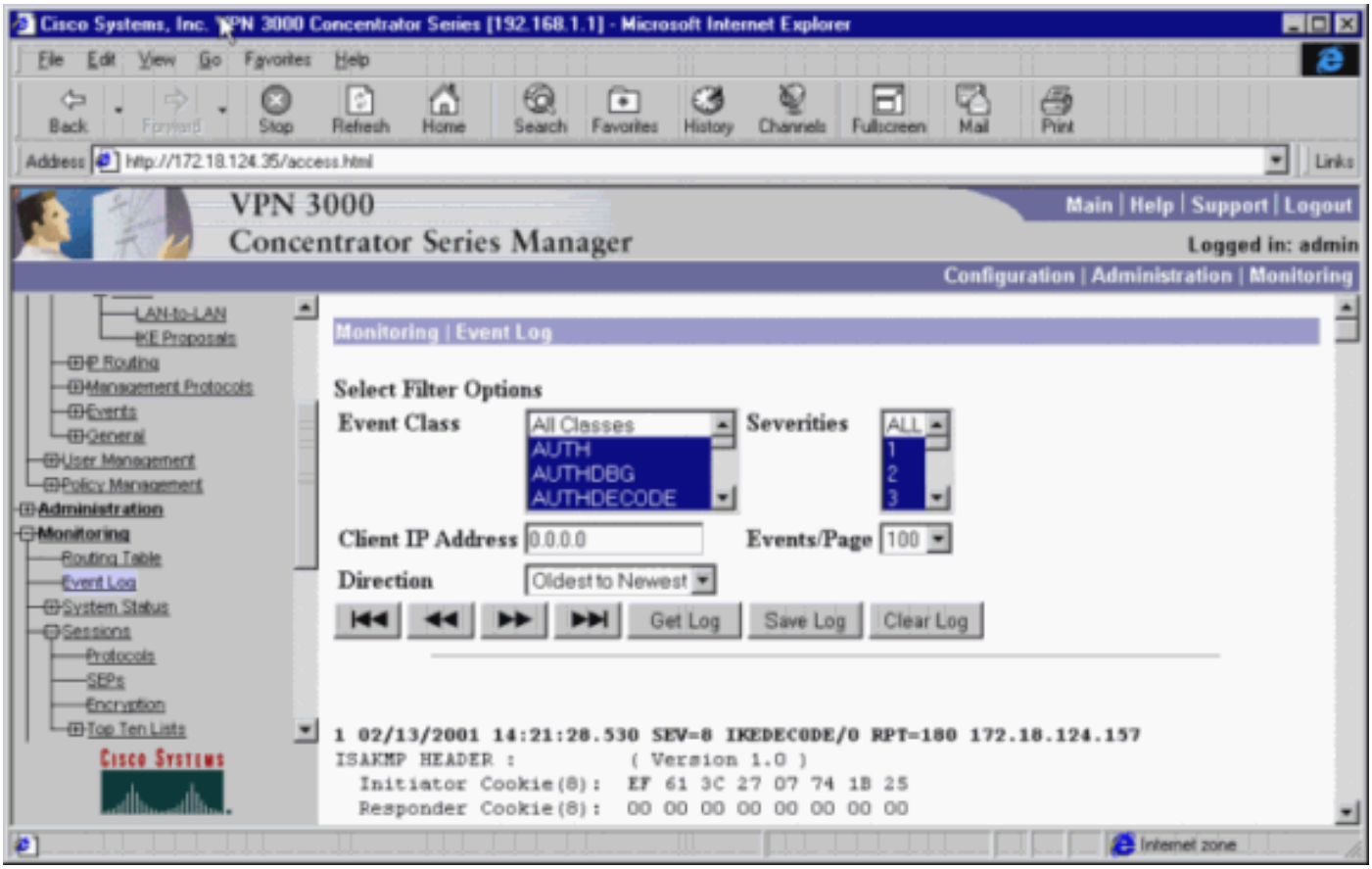
### تصحيح أخطاء مركز VPN 3000

تتضمن عمليات تصحيح أخطاء مركز الشبكة الخاصة الظاهرية (VPN) المحتملة IKE و iKEDBG و iKedecode و IPSec و IPSECDBG و IPSECDECODE. ويتم إعداد هذا في **التكوين > النظام > الأحداث > الفئات**.

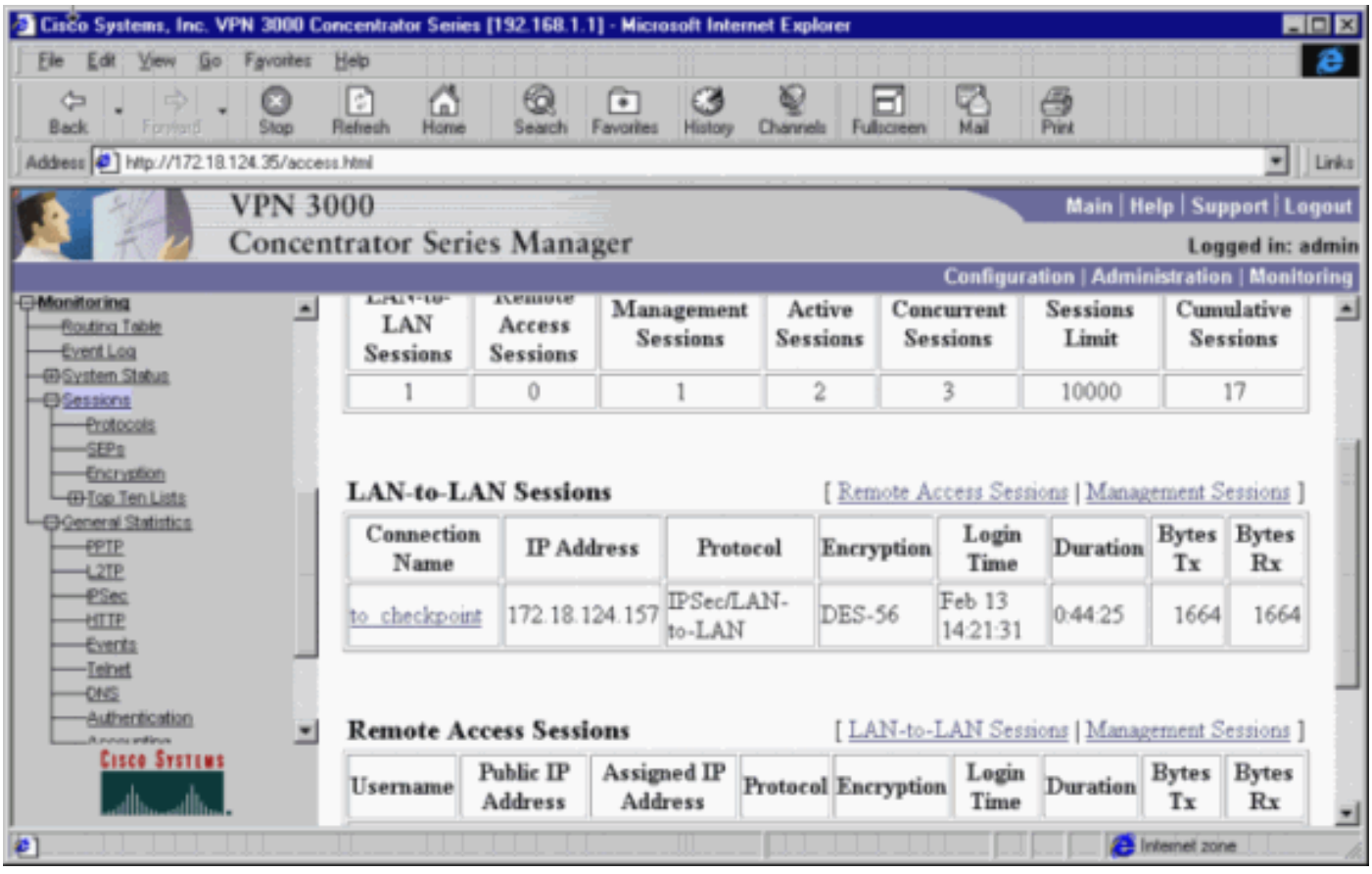

Cisco Systems, Inc. VPN 3000 Concentrator Series [192.168.1.1] - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: http://172.18.124.35/access.html
What's Related
Instant Message WebMail Contact People Yellow Pages Download Channels
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
Servers
Address Management
Tunneling Protocols
PPTP
L2TP
IPSec
LAN-to-LAN
IKE Proposals
IP Routing
Management Protocols
Events
General
FTP Backup
Classes
Trap Destinations
Syslog Servers
SMTP Servers
Email Recipients
General
User Management
Policy Management
Access Hours
Traffic Management
Network Lists
Cisco Systems
Configuration | System | Events | Classes
Save
This section lets you configure special handling of specific event classes.
Click the Add button to add an event class, or select an event class and click Modify or Delete.
Click here to configure general event parameters.
Configured Event Classes
Actions
IKE
IKEDBG
IKEDECODE
IPSEC
IPSECDBG
IPSECDECODE
Add
Modify
Delete
Click to collapse nested items




يمكنك عرض تصحيح الأخطاء في **المراقبة > سجل الأحداث > الحصول على سجل**.




حدد **مراقبة > جلسات العمل** لمراقبة حركة مرور نفق من شبكة LAN إلى شبكة LAN.




حدد **إدارة > إدارة الجلسات > جلسات عمل شبكة LAN > الإجراءات - تسجيل الخروج** لمسح النفق.

## تصحيح أخطاء جدار الحماية Checkpoint 4.1

**ملاحظة:** كان هذا تثبيت Microsoft Windows NT. نظرا لأنه تم تعيين التعقب لفترة طويلة في نافذة محرر النهج، يجب أن تظهر حركة المرور المرفوضة باللون الأحمر في عارض السجل. يمكن الحصول على المزيد من تصحيح الأخطاء المطبعية مع:

```
C:\WINNT\FW1\4.1\fwstop
C:\WINNT\FW1\4.1\fw d -d
```

وفي نافذة تانية:

```
C:\WINNT\FW1\4.1\fwstart
```

أصدرت هذا أمر أن يمسح SAs على التفتيش:

```
fw tab -t IKE_SA_table -x
fw tab -t ISAKMP_ESP_table -x
fw tab -t inbound_SPI -x
fw tab -t ISAKMP_AH_table -x
```

أجب **بنعم** في ؟

## إخراج تصحيح الأخطاء للعينة

### مركز Cisco VPN 3000

```
SEV=8 IKEDECODE/0 RPT=180 172.18.124.157 14:21:28.530 02/13/2001 1
                          ( ISAKMP HEADER :         ( Version 1.0
                  Initiator Cookie(8):  EF 61 3C 27 07 74 1B 25
                  Responder Cookie(8):  00 00 00 00 00 00 00 00
                                  (Next Payload  :       SA (1
                        Exchange Type :       Oakley Main Mode
                                       Flags         :       0
                                       Message ID    :       0
                                     Length        :       164

   SEV=8 IKEDBG/0 RPT=406 172.18.124.157 14:21:28.530 02/13/2001 7
                       : RECEIVED Message (msgid=0) with payloads
      HDR + SA (1) + VENDOR (13) + NONE (0) ... total length : 164

   SEV=9 IKEDBG/0 RPT=407 172.18.124.157 14:21:28.530 02/13/2001 9
                                          processing SA payload

SEV=8 IKEDECODE/0 RPT=181 172.18.124.157 14:21:28.530 02/13/2001 10
                                          : SA Payload Decode
                                  (DOI           :       IPSEC (1
                             (Situation     :       Identity Only (1
                                          Length        :       92

SEV=8 IKEDECODE/0 RPT=182 172.18.124.157 14:21:28.530 02/13/2001 13
                                            :Proposal Decode
                                           Proposal #    :       1
                                  (Protocol ID   :       ISAKMP (1
                                           of Transforms:       2#
                                          Length        :       80

SEV=8 IKEDECODE/0 RPT=183 172.18.124.157 14:21:28.530 02/13/2001 16
                                  :Transform # 1 Decode for Proposal # 1
```

```
                                        Transform #   :       1
                                    (Transform ID  :       IKE (1
                                         Length        :       36

SEV=8 IKEDECODE/0 RPT=184 172.18.124.157 14:21:28.530 02/13/2001 18
                        :Phase 1 SA Attribute Decode for Transform # 1
                                  (Encryption Alg:       DES-CBC (1
                                      (Hash Alg      :       SHA (2
                               (Auth Method   :       Preshared Key (1
                              (DH Group      :       Oakley Group 2 (2
                                   Life Time     :       86400 seconds

SEV=8 IKEDECODE/0 RPT=185 172.18.124.157 14:21:28.530 02/13/2001 23
                                :Transform # 2 Decode for Proposal # 1
                                        Transform #   :       2
                                    (Transform ID  :       IKE (1
                                         Length        :       36

SEV=8 IKEDECODE/0 RPT=186 172.18.124.157 14:21:28.530 02/13/2001 25
                        :Phase 1 SA Attribute Decode for Transform # 2
                                  (Encryption Alg:       DES-CBC (1
                                      (Hash Alg      :       SHA (2
                               (Auth Method   :       Preshared Key (1
                              (DH Group      :       Oakley Group 1 (1
                                   Life Time     :       86400 seconds

   SEV=8 IKEDBG/0 RPT=408 172.18.124.157 14:21:28.530 02/13/2001 30
                    Proposal # 1, Transform # 1, Type ISAKMP, Id IKE
                                      :Parsing received transform
                  :Phase 1 failure against global IKE proposal # 1
                         :Mismatched attr types for class DH Group
                                       Rcv'd: Oakley Group 2
                                       Cfg'd: Oakley Group 1

   SEV=8 IKEDBG/0 RPT=409 172.18.124.157 14:21:28.530 02/13/2001 35
                  :Phase 1 failure against global IKE proposal # 2
                         :Mismatched attr types for class DH Group
                                       Rcv'd: Oakley Group 2
                                       Cfg'd: Oakley Group 1

   SEV=8 IKEDBG/0 RPT=410 172.18.124.157 14:21:28.530 02/13/2001 38
                  :Phase 1 failure against global IKE proposal # 3
                   :Mismatched attr types for class Encryption Alg
                                            Rcv'd: DES-CBC
                                        Cfg'd: Triple-DES

   SEV=7 IKEDBG/0 RPT=411 172.18.124.157 14:21:28.530 02/13/2001 41
                                     Oakley proposal is acceptable

   SEV=9 IKEDBG/1 RPT=107 172.18.124.157 14:21:28.530 02/13/2001 42
                                          processing vid payload

   SEV=9 IKEDBG/0 RPT=412 172.18.124.157 14:21:28.530 02/13/2001 43
                                            processing IKE SA

   SEV=8 IKEDBG/0 RPT=413 172.18.124.157 14:21:28.530 02/13/2001 44
                    Proposal # 1, Transform # 1, Type ISAKMP, Id IKE
                                      :Parsing received transform
                  :Phase 1 failure against global IKE proposal # 1
                         :Mismatched attr types for class DH Group
                                       Rcv'd: Oakley Group 2
                                       Cfg'd: Oakley Group 1

   SEV=8 IKEDBG/0 RPT=414 172.18.124.157 14:21:28.530 02/13/2001 49
```

```
                                    :Phase 1 failure against global IKE proposal # 2
                                           :Mismatched attr types for class DH Group
                                                                Rcv'd: Oakley Group 2
                                                                Cfg'd: Oakley Group 1

                          SEV=8 IKEDBG/0 RPT=415 172.18.124.157 14:21:28.530 02/13/2001 52
                                       :Phase 1 failure against global IKE proposal # 3
                                        :Mismatched attr types for class Encryption Alg
                                                                    Rcv'd: DES-CBC
                                                                 Cfg'd: Triple-DES

                           SEV=7 IKEDBG/28 RPT=3 172.18.124.157 14:21:28.530 02/13/2001 55
                                           IKE SA Proposal # 1, Transform # 2 acceptable
                                                        Matches global IKE entry # 1

                          SEV=9 IKEDBG/0 RPT=416 172.18.124.157 14:21:28.530 02/13/2001 56
                                                     constructing ISA_SA for isakmp

                          SEV=8 IKEDBG/0 RPT=417 172.18.124.157 14:21:28.530 02/13/2001 57
                                                : SENDING Message (msgid=0) with payloads
                                                     HDR + SA (1)  ... total length : 84

                        SEV=8 IKEDECODE/0 RPT=187 172.18.124.157 14:21:28.630 02/13/2001 58
                                                    ( ISAKMP HEADER :         ( Version 1.0
                                              Initiator Cookie(8):  EF 61 3C 27 07 74 1B 25
                                              Responder Cookie(8):  24 18 40 A1 3B E4 95 26
                                                           (Next Payload  :       KE (4
                                                  Exchange Type :       Oakley Main Mode
                                                                Flags         :       0
                                                                Message ID    :       0
                                                             Length        :       152

                          SEV=8 IKEDBG/0 RPT=418 172.18.124.157 14:21:28.630 02/13/2001 64
                                                : RECEIVED Message (msgid=0) with payloads
                               HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152

                          SEV=8 IKEDBG/0 RPT=419 172.18.124.157 14:21:28.630 02/13/2001 66
                                                : RECEIVED Message (msgid=0) with payloads
                               HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152

                          SEV=9 IKEDBG/0 RPT=420 172.18.124.157 14:21:28.630 02/13/2001 68
                                                                processing ke payload

                          SEV=9 IKEDBG/0 RPT=421 172.18.124.157 14:21:28.630 02/13/2001 69
                                                                  processing ISA_KE

                          SEV=9 IKEDBG/1 RPT=108 172.18.124.157 14:21:28.630 02/13/2001 70
                                                              processing nonce payload

                          SEV=9 IKEDBG/0 RPT=422 172.18.124.157 14:21:28.650 02/13/2001 71
                                                               constructing ke payload

                          SEV=9 IKEDBG/1 RPT=109 172.18.124.157 14:21:28.650 02/13/2001 72
                                                             constructing nonce payload

                           SEV=9 IKEDBG/38 RPT=7 172.18.124.157 14:21:28.650 02/13/2001 73
        Constructing VPN 3000 spoofing IOS Vendor ID payload (version: 1.0.0, capabiliti
                                                                            (es: 20000001

                          SEV=9 IKEDBG/1 RPT=110 172.18.124.157 14:21:28.650 02/13/2001 75
                                                               constructing vid payload

                             SEV=9 IKE/0 RPT=26 172.18.124.157 14:21:28.650 02/13/2001 76
                                                          ...Generating keys for Responder
```

```
   SEV=8 IKEDBG/0 RPT=423 172.18.124.157 14:21:28.650 02/13/2001 77
                          : SENDING Message (msgid=0) with payloads
                               HDR + KE (4)  ... total length : 192

SEV=8 IKEDECODE/0 RPT=188 172.18.124.157 14:21:28.770 02/13/2001 78
                            ( ISAKMP HEADER :         ( Version 1.0
                    Initiator Cookie(8):  EF 61 3C 27 07 74 1B 25
                    Responder Cookie(8):  24 18 40 A1 3B E4 95 26
                                    (Next Payload  :       ID (5
                           Exchange Type :       Oakley Main Mode
                             ( Flags         :       1   (ENCRYPT
                                         Message ID    :       0
                                        Length        :       68

   SEV=8 IKEDBG/0 RPT=424 172.18.124.157 14:21:28.770 02/13/2001 84
                         : RECEIVED Message (msgid=0) with payloads
          HDR + ID (5) + HASH (8) + NONE (0) ... total length : 64

   SEV=9 IKEDBG/1 RPT=111 172.18.124.157 14:21:28.770 02/13/2001 86
                                                    Processing ID

   SEV=9 IKEDBG/0 RPT=425 172.18.124.157 14:21:28.770 02/13/2001 87
                                                  processing hash

   SEV=9 IKEDBG/0 RPT=426 172.18.124.157 14:21:28.770 02/13/2001 88
                                                  computing hash

    SEV=9 IKEDBG/23 RPT=7 172.18.124.157 14:21:28.770 02/13/2001 89
                        Starting group lookup for peer 172.18.124.157

   SEV=7 IKEDBG/0 RPT=427 172.18.124.157 14:21:28.870 02/13/2001 90
                               (Found Phase 1 Group (172.18.124.157

    SEV=7 IKEDBG/14 RPT=7 172.18.124.157 14:21:28.870 02/13/2001 91
                             Authentication configured for Internal

   SEV=9 IKEDBG/1 RPT=112 172.18.124.157 14:21:28.870 02/13/2001 92
                                                  constructing ID

                    SEV=9 IKEDBG/0 RPT=428 14:21:28.870 02/13/2001 93
                                              construct hash payload

   SEV=9 IKEDBG/0 RPT=429 172.18.124.157 14:21:28.870 02/13/2001 94
                                                  computing hash


   SEV=8 IKEDBG/0 RPT=430 172.18.124.157 14:21:28.870 02/13/2001 95
                          : SENDING Message (msgid=0) with payloads
                               HDR + ID (5)  ... total length : 64

   SEV=7 IKEDBG/0 RPT=431 172.18.124.157 14:21:28.870 02/13/2001 96
                                        Starting phase 1 rekey timer

SEV=8 IKEDECODE/0 RPT=189 172.18.124.157 14:21:29.030 02/13/2001 97
                            ( ISAKMP HEADER :         ( Version 1.0
                    Initiator Cookie(8):  EF 61 3C 27 07 74 1B 25
                    Responder Cookie(8):  24 18 40 A1 3B E4 95 26
                                   (Next Payload  :       HASH (8
                          Exchange Type :       Oakley Quick Mode
                             ( Flags         :       1   (ENCRYPT
                                   Message ID    :       7755aa11
                                        Length        :       164
```

```
                SEV=8 IKEDBG/0 RPT=432 172.18.124.157 14:21:29.030 02/13/2001 104
                                : RECEIVED Message (msgid=7755aa11) with payloads
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) ... total leng
                                                                        th : 160

                SEV=9 IKEDBG/0 RPT=433 172.18.124.157 14:21:29.030 02/13/2001 107
                                                              processing hash

                SEV=9 IKEDBG/0 RPT=434 172.18.124.157 14:21:29.030 02/13/2001 108
                                                          processing SA payload

             SEV=8 IKEDECODE/0 RPT=190 172.18.124.157 14:21:29.030 02/13/2001 109
                                                          : SA Payload Decode
                                          (DOI           :       IPSEC (1
                                 (Situation     :       Identity Only (1
                                                Length        :       52

             SEV=8 IKEDECODE/0 RPT=191 172.18.124.157 14:21:29.030 02/13/2001 112
                                                        :Proposal Decode
                                                Proposal #    :       1
                                       (Protocol ID   :       ESP (3
                                                of Transforms:       1#
                                     Spi           :       DA 16 3F E3
                                                Length        :       40

             SEV=8 IKEDECODE/0 RPT=192 172.18.124.157 14:21:29.030 02/13/2001 116
                                  :Transform # 1 Decode for Proposal # 1
                                                Transform #   :       1
                                     (Transform ID  :       DES-CBC (2
                                                Length        :       28

             SEV=8 IKEDECODE/0 RPT=193 172.18.124.157 14:21:29.030 02/13/2001 118
                             :Phase 2 SA Attribute Decode for Transform # 1
                                      Life Time     :       28800 seconds
                                           (HMAC Algorithm:       SHA (2
                                       (Encapsulation :       Tunnel (1

                SEV=9 IKEDBG/1 RPT=113 172.18.124.157 14:21:29.030 02/13/2001 121
                                                        processing nonce payload

                SEV=9 IKEDBG/1 RPT=114 172.18.124.157 14:21:29.030 02/13/2001 122
                                                              Processing ID

                   SEV=5 IKE/35 RPT=14 172.18.124.157 14:21:29.030 02/13/2001 123
                              :Received remote IP Proxy Subnet data in ID Payload
                     Address 10.32.50.0, Mask 255.255.255.0, Protocol 0, Port 0

                SEV=9 IKEDBG/1 RPT=115 172.18.124.157 14:21:29.030 02/13/2001 125
                                                              Processing ID

                   SEV=5 IKE/34 RPT=14 172.18.124.157 14:21:29.030 02/13/2001 126
                              :Received local IP Proxy Subnet data in ID Payload
                    Address 192.168.1.0, Mask 255.255.255.0, Protocol 0, Port 0

                    SEV=5 IKE/66 RPT=4 172.18.124.157 14:21:29.030 02/13/2001 128
                            IKE Remote Peer configured for SA: L2L: to_checkpoint

                SEV=9 IKEDBG/0 RPT=435 172.18.124.157 14:21:29.030 02/13/2001 129
                                                          processing IPSEC SA

                 SEV=7 IKEDBG/27 RPT=1 172.18.124.157 14:21:29.030 02/13/2001 130
                                  IPSec SA Proposal # 1, Transform # 1 acceptable

                SEV=7 IKEDBG/0 RPT=436 172.18.124.157 14:21:29.030 02/13/2001 131
```

```
                                                    !IKE: requesting SPI

                                SEV=8 IKEDBG/6 RPT=6 14:21:29.030 02/13/2001 132
                                   IKE got SPI from key engine: SPI = 0x4d6e483f

                              SEV=9 IKEDBG/0 RPT=437 172.18.124.157 14:21:29.030 02/13/2001 133
                                                    oakley constucting quick mode

                              SEV=9 IKEDBG/0 RPT=438 172.18.124.157 14:21:29.030 02/13/2001 134
                                                        constructing blank hash

                              SEV=9 IKEDBG/0 RPT=439 172.18.124.157 14:21:29.030 02/13/2001 135
                                                    constructing ISA_SA for ipsec

                              SEV=9 IKEDBG/1 RPT=116 172.18.124.157 14:21:29.030 02/13/2001 136
                                                  constructing ipsec nonce payload

                              SEV=9 IKEDBG/1 RPT=117 172.18.124.157 14:21:29.030 02/13/2001 137
                                                        constructing proxy ID

                              SEV=7 IKEDBG/0 RPT=440 172.18.124.157 14:21:29.030 02/13/2001 138
                                                       :Transmitting Proxy Id
                               Remote subnet: 10.32.50.0  Mask 255.255.255.0 Protocol 0  Port 0
                              Local subnet:  192.168.1.0  mask 255.255.255.0 Protocol 0  Port 0

                              SEV=9 IKEDBG/0 RPT=441 172.18.124.157 14:21:29.030 02/13/2001 141
                                                        constructing qm hash

                              SEV=8 IKEDBG/0 RPT=442 172.18.124.157 14:21:29.030 02/13/2001 142
                                   : SENDING Message (msgid=7755aa11) with payloads
                                             HDR + HASH (8)  ... total length : 156

                            SEV=8 IKEDECODE/0 RPT=194 172.18.124.157 14:21:29.270 02/13/2001 144
                                                ( ISAKMP HEADER :         ( Version 1.0
                                      Initiator Cookie(8):  EF 61 3C 27 07 74 1B 25
                                      Responder Cookie(8):  24 18 40 A1 3B E4 95 26
                                                    (Next Payload  :       HASH (8
                                           Exchange Type :       Oakley Quick Mode
                                              ( Flags         :       1   (ENCRYPT
                                                    Message ID    :       7755aa11
                                                          Length        :       60

                              SEV=8 IKEDBG/0 RPT=443 172.18.124.157 14:21:29.270 02/13/2001 151
                                   : RECEIVED Message (msgid=7755aa11) with payloads
                                     HDR + HASH (8) + NONE (0) ... total length : 52

                              SEV=9 IKEDBG/0 RPT=444 172.18.124.157 14:21:29.270 02/13/2001 153
                                                                processing hash

                              SEV=9 IKEDBG/0 RPT=445 172.18.124.157 14:21:29.270 02/13/2001 154
                                                        loading all IPSEC SAs

                              SEV=9 IKEDBG/1 RPT=118 172.18.124.157 14:21:29.270 02/13/2001 155
                                                    !Generating Quick Mode Key

                              SEV=9 IKEDBG/1 RPT=119 172.18.124.157 14:21:29.270 02/13/2001 156
                                                    !Generating Quick Mode Key

                              SEV=7 IKEDBG/0 RPT=446 172.18.124.157 14:21:29.270 02/13/2001 157
                                                                 :Loading subnet
                                                Dst: 192.168.1.0  mask: 255.255.255.0
                                                 Src: 10.32.50.0  mask: 255.255.255.0

                                  SEV=4 IKE/49 RPT=6 172.18.124.157 14:21:29.270 02/13/2001 159
```

```
(Security negotiation complete for LAN-to-LAN Group (172.18.124.157
     Responder, Inbound SPI = 0x4d6e483f, Outbound SPI = 0xda163fe3

                    SEV=8 IKEDBG/7 RPT=6 14:21:29.270 02/13/2001 161
                      IKE got a KEY_ADD msg for SA: SPI = 0xda163fe3

                  SEV=8 IKEDBG/0 RPT=447 14:21:29.270 02/13/2001 162
                            pitcher: rcv KEY_UPDATE, spi 0x4d6e483f

SEV=8 IKEDECODE/0 RPT=195 172.18.124.157 14:21:29.670 02/13/2001 163
                            ( ISAKMP HEADER :         ( Version 1.0
                     Initiator Cookie(8):  EF 61 3C 27 07 74 1B 25
                     Responder Cookie(8):  24 18 40 A1 3B E4 95 26
                                  (Next Payload  :       HASH (8
                           Exchange Type :       Oakley Quick Mode
                              ( Flags         :       1   (ENCRYPT
                                    Message ID    :       7755aa11
                                          Length        :       60

       SEV=6 IKE/0 RPT=27 172.18.124.157 14:21:29.670 02/13/2001 170
                                !Duplicate Phase 2 packet detected

SEV=8 IKEDECODE/0 RPT=196 172.18.124.157 14:21:29.760 02/13/2001 171
                            ( ISAKMP HEADER :         ( Version 1.0
                     Initiator Cookie(8):  EF 61 3C 27 07 74 1B 25
                     Responder Cookie(8):  24 18 40 A1 3B E4 95 26
                                  (Next Payload  :       HASH (8
                           Exchange Type :       Oakley Quick Mode
                              ( Flags         :       1   (ENCRYPT
                                    Message ID    :       7755aa11
                                          Length        :       60

       SEV=6 IKE/0 RPT=28 172.18.124.157 14:21:29.760 02/13/2001 178
                                !Duplicate Phase 2 packet detected

                  SEV=8 IKEDBG/0 RPT=448 14:21:29.880 02/13/2001 179
                          pitcher: recv KEY_SA_ACTIVE spi 0x4d6e483f

                  SEV=8 IKEDBG/0 RPT=449 14:21:29.880 02/13/2001 180
        KEY_SA_ACTIVE old rekey centry found with new spi 0x4d6e483f

    SEV=7 IKEDBG/9 RPT=5 172.18.124.157 14:21:29.880 02/13/2001 181
  IKE Deleting SA: Remote Proxy 10.32.50.0, Local Proxy 192.168.1.0

  SEV=9 IKEDBG/0 RPT=450 172.18.124.157 14:21:29.880 02/13/2001 182
          IKE SA MM:f2ea8e68 rcv'd Terminate: state MM_ACTIVE_REKEY
                              flags 0x000000e6, refcnt 1, tuncnt 0

  SEV=9 IKEDBG/0 RPT=451 172.18.124.157 14:21:29.880 02/13/2001 184
                                   :IKE SA MM:f2ea8e68 terminating
                              flags 0x000000a6, refcnt 0, tuncnt 0

                  SEV=9 IKEDBG/0 RPT=452 14:21:29.880 02/13/2001 185
                                          sending delete message

  SEV=9 IKEDBG/0 RPT=453 172.18.124.157 14:21:29.880 02/13/2001 186
                                        constructing blank hash

                  SEV=9 IKEDBG/0 RPT=454 14:21:29.880 02/13/2001 187
                                      constructing delete payload

  SEV=9 IKEDBG/0 RPT=455 172.18.124.157 14:21:29.880 02/13/2001 188
                                          constructing qm hash
```

```
SEV=8 IKEDBG/0 RPT=456 172.18.124.157 14:21:29.880 02/13/2001 189
: SENDING Message (msgid=87b7c1a4) with payloads
HDR + HASH (8)  ... total length : 80

SEV=9 IKEDBG/0 RPT=457 172.18.124.157 14:21:29.880 02/13/2001 191
IKE SA MM:241840a1 rcv'd Terminate: state MM_REKEY_DONE
flags 0x00000082, refcnt 1, tuncnt 1

SEV=6 IKE/0 RPT=29 172.18.124.157 14:21:29.880 02/13/2001 193
!Removing peer from peer table failed, no match

SEV=9 IKEDBG/0 RPT=458 14:21:29.880 02/13/2001 194
sending delete message

SEV=9 IKEDBG/0 RPT=459 172.18.124.157 14:21:29.880 02/13/2001 195
constructing blank hash

SEV=9 IKEDBG/0 RPT=460 14:21:29.880 02/13/2001 196
constructing ipsec delete payload

SEV=9 IKEDBG/0 RPT=461 172.18.124.157 14:21:29.880 02/13/2001 197
constructing qm hash

SEV=8 IKEDBG/0 RPT=462 172.18.124.157 14:21:29.880 02/13/2001 198
: SENDING Message (msgid=63f2abb8) with payloads
HDR + HASH (8)  ... total length : 68

SEV=7 IKEDBG/9 RPT=6 172.18.124.157 14:21:29.880 02/13/2001 200
IKE Deleting SA: Remote Proxy 10.32.50.0, Local Proxy 192.168.1.0

SEV=9 IKEDBG/0 RPT=463 172.18.124.157 14:21:29.880 02/13/2001 201
:IKE SA MM:241840a1 terminating
flags 0x00000082, refcnt 0, tuncnt 0

SEV=9 IKEDBG/0 RPT=464 14:21:29.880 02/13/2001 202
sending delete message

SEV=9 IKEDBG/0 RPT=465 172.18.124.157 14:21:29.880 02/13/2001 203
constructing blank hash

SEV=9 IKEDBG/0 RPT=466 14:21:29.880 02/13/2001 204
constructing delete payload

SEV=9 IKEDBG/0 RPT=467 172.18.124.157 14:21:29.880 02/13/2001 205
constructing qm hash

SEV=8 IKEDBG/0 RPT=468 172.18.124.157 14:21:29.880 02/13/2001 206
: SENDING Message (msgid=d6a00071) with payloads
HDR + HASH (8)  ... total length : 80

SEV=4 AUTH/22 RPT=13 14:21:29.880 02/13/2001 208
User 172.18.124.157 disconnected

SEV=8 IKEDBG/0 RPT=469 14:21:29.880 02/13/2001 209
pitcher: received key delete msg, spi 0x2962069b

SEV=8 IKEDBG/0 RPT=470 14:21:29.880 02/13/2001 210
pitcher: received key delete msg, spi 0xda163fe2

SEV=8 IKEDBG/0 RPT=471 14:21:29.880 02/13/2001 211
pitcher: received key delete msg, spi 0x4d6e483f

SEV=8 IKEDBG/0 RPT=472 14:21:29.880 02/13/2001 212
pitcher: received key delete msg, spi 0xda163fe3
```

```
                    SEV=8 IKEDBG/0 RPT=473 14:21:29.890 02/13/2001 213
                              !pitcher: received a key acquire message

        SEV=4 IKE/41 RPT=6 172.18.124.157 14:21:29.890 02/13/2001 214
          IKE Initiator: New Phase 1, Intf 2, IKE Peer 172.18.124.157
   ,local Proxy Address 192.168.1.0, remote Proxy Address 10.32.50.0
                                        (SA (L2L: to_checkpoint

   SEV=9 IKEDBG/0 RPT=474 172.18.124.157 14:21:29.890 02/13/2001 217
                                    constructing ISA_SA for isakmp

   SEV=8 IKEDBG/0 RPT=475 172.18.124.157 14:21:29.890 02/13/2001 218
                           : SENDING Message (msgid=0) with payloads
                                HDR + SA (1)  ... total length : 84

SEV=8 IKEDECODE/0 RPT=197 172.18.124.157 14:21:30.430 02/13/2001 219
                             ( ISAKMP HEADER :         ( Version 1.0
                      Initiator Cookie(8):  FE 75 39 26 66 21 F6 F8
                      Responder Cookie(8):  67 1D 73 71 AE 2B 88 2E
                                    (Next Payload  :       SA (1
                             Exchange Type :       Oakley Main Mode
                                    Flags         :       0
                                    Message ID    :       0
                                   Length        :       84

   SEV=8 IKEDBG/0 RPT=476 172.18.124.157 14:21:30.430 02/13/2001 225
                           : RECEIVED Message (msgid=0) with payloads
                         HDR + SA (1) + NONE (0) ... total length : 84

   SEV=8 IKEDBG/0 RPT=477 172.18.124.157 14:21:30.430 02/13/2001 227
                           : RECEIVED Message (msgid=0) with payloads
                         HDR + SA (1) + NONE (0) ... total length : 84

   SEV=9 IKEDBG/0 RPT=478 172.18.124.157 14:21:30.430 02/13/2001 229
                                               processing SA payload

SEV=8 IKEDECODE/0 RPT=198 172.18.124.157 14:21:30.430 02/13/2001 230
                                                  : SA Payload Decode
                                      (DOI           :       IPSEC (1
                                (Situation     :       Identity Only (1
                                               Length        :       56

SEV=8 IKEDECODE/0 RPT=199 172.18.124.157 14:21:30.430 02/13/2001 233
                                                     :Proposal Decode
                                               Proposal #    :       1
                                     (Protocol ID   :       ISAKMP (1
                                               of Transforms:       1#
                                               Length        :       44

SEV=8 IKEDECODE/0 RPT=200 172.18.124.157 14:21:30.430 02/13/2001 236
                                  :Transform # 1 Decode for Proposal # 1
                                               Transform #   :       1
                                        (Transform ID  :       IKE (1
                                               Length        :       36

SEV=8 IKEDECODE/0 RPT=201 172.18.124.157 14:21:30.440 02/13/2001 238
                            :Phase 1 SA Attribute Decode for Transform # 1
                                          (Encryption Alg:       DES-CBC (1
                                              (Hash Alg      :       SHA (2
                                 (DH Group      :       Oakley Group 1 (1
                                  (Auth Method   :       Preshared Key (1
                                      Life Time     :       86400 seconds
```

```
                    SEV=7 IKEDBG/0 RPT=479 172.18.124.157 14:21:30.440 02/13/2001 243
                                                Oakley proposal is acceptable

                    SEV=9 IKEDBG/0 RPT=480 172.18.124.157 14:21:30.440 02/13/2001 244
                                                  constructing ke payload

                    SEV=9 IKEDBG/1 RPT=120 172.18.124.157 14:21:30.440 02/13/2001 245
                                                constructing nonce payload

                     SEV=9 IKEDBG/38 RPT=8 172.18.124.157 14:21:30.440 02/13/2001 246
Constructing VPN 3000 spoofing IOS Vendor ID payload (version: 1.0.0, capabiliti
                                                                      (es: 20000001

                    SEV=9 IKEDBG/1 RPT=121 172.18.124.157 14:21:30.440 02/13/2001 248
                                                  constructing vid payload

                    SEV=8 IKEDBG/0 RPT=481 172.18.124.157 14:21:30.440 02/13/2001 249
                                  : SENDING Message (msgid=0) with payloads
                                       HDR + KE (4)  ... total length : 192

                SEV=8 IKEDECODE/0 RPT=202 172.18.124.157 14:21:30.540 02/13/2001 250
                                     ( ISAKMP HEADER :         ( Version 1.0
                               Initiator Cookie(8):  FE 75 39 26 66 21 F6 F8
                               Responder Cookie(8):  67 1D 73 71 AE 2B 88 2E
                                            (Next Payload  :       KE (4
                                   Exchange Type :       Oakley Main Mode
                                                 Flags         :       0
                                                 Message ID    :       0
                                              Length        :       152

                    SEV=8 IKEDBG/0 RPT=482 172.18.124.157 14:21:30.540 02/13/2001 256
                                  : RECEIVED Message (msgid=0) with payloads
                          HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152

                    SEV=8 IKEDBG/0 RPT=483 172.18.124.157 14:21:30.540 02/13/2001 258
                                  : RECEIVED Message (msgid=0) with payloads
                          HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152

                    SEV=9 IKEDBG/0 RPT=484 172.18.124.157 14:21:30.540 02/13/2001 260
                                                  processing ke payload

                    SEV=9 IKEDBG/0 RPT=485 172.18.124.157 14:21:30.540 02/13/2001 261
                                                       processing ISA_KE

                    SEV=9 IKEDBG/1 RPT=122 172.18.124.157 14:21:30.540 02/13/2001 262
                                                  processing nonce payload

                        SEV=9 IKE/0 RPT=30 172.18.124.157 14:21:30.560 02/13/2001 263
                                            ...Generating keys for Initiator

                    SEV=9 IKEDBG/1 RPT=123 172.18.124.157 14:21:30.570 02/13/2001 264
                                                       constructing ID

                                SEV=9 IKEDBG/0 RPT=486 14:21:30.570 02/13/2001 265
                                                  construct hash payload

                    SEV=9 IKEDBG/0 RPT=487 172.18.124.157 14:21:30.570 02/13/2001 266
                                                       computing hash

                    SEV=8 IKEDBG/0 RPT=488 172.18.124.157 14:21:30.570 02/13/2001 267
                                  : SENDING Message (msgid=0) with payloads
                                       HDR + ID (5)  ... total length : 64

                SEV=8 IKEDECODE/0 RPT=203 172.18.124.157 14:21:30.740 02/13/2001 268
```

```
                                ( ISAKMP HEADER :         ( Version 1.0
                          Initiator Cookie(8):  FE 75 39 26 66 21 F6 F8
                          Responder Cookie(8):  67 1D 73 71 AE 2B 88 2E
                                          (Next Payload  :       ID (5
                                 Exchange Type :       Oakley Main Mode
                                   ( Flags         :       1   (ENCRYPT
                                               Message ID    :       0
                                              Length        :       68

   SEV=8 IKEDBG/0 RPT=489 172.18.124.157 14:21:30.740 02/13/2001 274
                                : RECEIVED Message (msgid=0) with payloads
            HDR + ID (5) + HASH (8) + NONE (0) ... total length : 64

   SEV=9 IKEDBG/1 RPT=124 172.18.124.157 14:21:30.740 02/13/2001 276
                                                        Processing ID

   SEV=9 IKEDBG/0 RPT=490 172.18.124.157 14:21:30.740 02/13/2001 277
                                                     processing hash

   SEV=9 IKEDBG/0 RPT=491 172.18.124.157 14:21:30.740 02/13/2001 278
                                                     computing hash

    SEV=9 IKEDBG/23 RPT=8 172.18.124.157 14:21:30.740 02/13/2001 279
                           Starting group lookup for peer 172.18.124.157

SEV=8 IKEDECODE/0 RPT=204 172.18.124.157 14:21:30.830 02/13/2001 280
                                ( ISAKMP HEADER :         ( Version 1.0
                          Initiator Cookie(8):  FE 75 39 26 66 21 F6 F8
                          Responder Cookie(8):  67 1D 73 71 AE 2B 88 2E
                                          (Next Payload  :       ID (5
                                 Exchange Type :       Oakley Main Mode
                                   ( Flags         :       1   (ENCRYPT
                                               Message ID    :       0
                                              Length        :       68

       SEV=6 IKE/0 RPT=31 172.18.124.157 14:21:30.830 02/13/2001 286
                                    !Duplicate Phase 1 packet detected

                         SEV=6 IKE/0 RPT=32 14:21:30.830 02/13/2001 287
       MM received unexpected event EV_RESEND_MSG in state MM_I_DONE

   SEV=7 IKEDBG/0 RPT=492 172.18.124.157 14:21:30.840 02/13/2001 288
                                   (Found Phase 1 Group (172.18.124.157

    SEV=7 IKEDBG/14 RPT=8 172.18.124.157 14:21:30.840 02/13/2001 289
                                   Authentication configured for Internal

   SEV=9 IKEDBG/0 RPT=493 172.18.124.157 14:21:30.840 02/13/2001 290
                                               Oakley begin quick mode

   SEV=7 IKEDBG/0 RPT=494 172.18.124.157 14:21:30.840 02/13/2001 291
                                          Starting phase 1 rekey timer

                        SEV=4 AUTH/21 RPT=15 14:21:30.840 02/13/2001 292
                                          User 172.18.124.157 connected

                        SEV=8 IKEDBG/6 RPT=7 14:21:30.840 02/13/2001 293
                           IKE got SPI from key engine: SPI = 0x08201539

   SEV=9 IKEDBG/0 RPT=495 172.18.124.157 14:21:30.840 02/13/2001 294
                                          oakley constucting quick mode

   SEV=9 IKEDBG/0 RPT=496 172.18.124.157 14:21:30.840 02/13/2001 295
                                               constructing blank hash
```

```
SEV=9 IKEDBG/0 RPT=497 172.18.124.157 14:21:30.840 02/13/2001 296
                                        constructing ISA_SA for ipsec

SEV=9 IKEDBG/1 RPT=125 172.18.124.157 14:21:30.840 02/13/2001 297
                                    constructing ipsec nonce payload

SEV=9 IKEDBG/1 RPT=126 172.18.124.157 14:21:30.840 02/13/2001 298
                                                 constructing proxy ID

SEV=7 IKEDBG/0 RPT=498 172.18.124.157 14:21:30.840 02/13/2001 299
                                                :Transmitting Proxy Id
 Local subnet:  192.168.1.0  mask 255.255.255.0 Protocol 0  Port 0
  Remote subnet: 10.32.50.0  Mask 255.255.255.0 Protocol 0  Port 0

SEV=9 IKEDBG/0 RPT=499 172.18.124.157 14:21:30.840 02/13/2001 302
                                                 constructing qm hash

SEV=8 IKEDBG/0 RPT=500 172.18.124.157 14:21:30.840 02/13/2001 303
                          : SENDING Message (msgid=23bc1709) with payloads
                                    HDR + HASH (8)  ... total length : 184

SEV=8 IKEDECODE/0 RPT=205 172.18.124.157 14:21:31.000 02/13/2001 305
                                  ( ISAKMP HEADER :         ( Version 1.0
                             Initiator Cookie(8):  FE 75 39 26 66 21 F6 F8
                             Responder Cookie(8):  67 1D 73 71 AE 2B 88 2E
                                        (Next Payload  :       HASH (8
                                   Exchange Type :       Oakley Quick Mode
                                      ( Flags         :       1   (ENCRYPT
                                            Message ID    :       23bc1709
                                                 Length        :       164

SEV=8 IKEDBG/0 RPT=501 172.18.124.157 14:21:31.000 02/13/2001 312
                          : RECEIVED Message (msgid=23bc1709) with payloads
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) ... total leng
                                                                        th : 156

SEV=9 IKEDBG/0 RPT=502 172.18.124.157 14:21:31.000 02/13/2001 315
                                                   processing hash

SEV=9 IKEDBG/0 RPT=503 172.18.124.157 14:21:31.000 02/13/2001 316
                                                 processing SA payload

SEV=8 IKEDECODE/0 RPT=206 172.18.124.157 14:21:31.000 02/13/2001 317
                                                     : SA Payload Decode
                                            (DOI           :       IPSEC (1
                                     (Situation     :       Identity Only (1
                                                 Length        :       48

SEV=8 IKEDECODE/0 RPT=207 172.18.124.157 14:21:31.000 02/13/2001 320
                                                       :Proposal Decode
                                                  Proposal #    :       1
                                             (Protocol ID   :       ESP (3
                                                  of Transforms:       1#
                                          Spi           :       DA 16 3F E4
                                                 Length        :       36

SEV=8 IKEDECODE/0 RPT=208 172.18.124.157 14:21:31.000 02/13/2001 324
                                       :Transform # 1 Decode for Proposal # 1
                                                  Transform #   :       1
                                          (Transform ID  :       DES-CBC (2
                                                 Length        :       24

SEV=8 IKEDECODE/0 RPT=209 172.18.124.157 14:21:31.000 02/13/2001 326
```

```
                                  :Phase 2 SA Attribute Decode for Transform # 1
                                           Life Time     :       28800 seconds
                                              (Encapsulation :       Tunnel (1
                                                 (HMAC Algorithm:       SHA (2

          SEV=9 IKEDBG/1 RPT=127 172.18.124.157 14:21:31.000 02/13/2001 329
                                                  processing nonce payload

          SEV=9 IKEDBG/1 RPT=128 172.18.124.157 14:21:31.000 02/13/2001 330
                                                        Processing ID

          SEV=9 IKEDBG/1 RPT=129 172.18.124.157 14:21:31.000 02/13/2001 331
                                                        Processing ID

          SEV=9 IKEDBG/0 RPT=504 172.18.124.157 14:21:31.000 02/13/2001 332
                                                     loading all IPSEC SAs

          SEV=9 IKEDBG/1 RPT=130 172.18.124.157 14:21:31.000 02/13/2001 333
                                                  !Generating Quick Mode Key

          SEV=9 IKEDBG/1 RPT=131 172.18.124.157 14:21:31.010 02/13/2001 334
                                                  !Generating Quick Mode Key

          SEV=7 IKEDBG/0 RPT=505 172.18.124.157 14:21:31.010 02/13/2001 335
                                                        :Loading subnet
                                       Dst: 10.32.50.0  mask: 255.255.255.0
                                      Src: 192.168.1.0  mask: 255.255.255.0

               SEV=4 IKE/49 RPT=7 172.18.124.157 14:21:31.010 02/13/2001 337
        (Security negotiation complete for LAN-to-LAN Group (172.18.124.157
             Initiator, Inbound SPI = 0x08201539, Outbound SPI = 0xda163fe4

          SEV=9 IKEDBG/0 RPT=506 172.18.124.157 14:21:31.010 02/13/2001 339
                                        oakley constructing final quick mode

          SEV=8 IKEDBG/0 RPT=507 172.18.124.157 14:21:31.010 02/13/2001 340
                           : SENDING Message (msgid=23bc1709) with payloads
                                     HDR + HASH (8)  ... total length : 76

                        SEV=8 IKEDBG/7 RPT=7 14:21:31.010 02/13/2001 342
                          IKE got a KEY_ADD msg for SA: SPI = 0xda163fe4

                       SEV=8 IKEDBG/0 RPT=508 14:21:31.010 02/13/2001 343
                                    pitcher: rcv KEY_UPDATE, spi 0x8201539

                       SEV=8 IKEDBG/0 RPT=509 14:21:31.890 02/13/2001 344
                                 pitcher: recv KEY_SA_ACTIVE spi 0x8201539

                       SEV=8 IKEDBG/0 RPT=510 14:21:31.890 02/13/2001 345
KEY_SA_ACTIVE no old rekey centry found with new spi 0x8201539, mess_id 0x0
```

## معلومات ذات صلة

- مفاوضة IPSec/بروتوكولات IKE
- 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).