ASA/PIX 7.x: مثال تكوين إرتباطات ISP المكررة والاحتياطية

المحتويات

المقدمة

توجد مشكلة في المسارات الثابتة تتمثل في عدم وجود آلية مدمجة لتحديد ما إذا كان المسار أعلى أو أسفل. يبقى المسار في جدول التوجيه حتى إذا أصبحت بوابة الخطوة التالية غير متوفرة. تتم إزالة المسارات الثابتة من جدول التوجيه فقط في حالة تعطل الواجهة المقترنة الموجودة على جهاز الأمان. لحل هذه المشكلة، يتم إستخدام ميزة تعقب المسار الثابت لتعقب توفر مسار ثابت، وإذا فشل هذا المسار، فعليك إزالته من جدول التوجيه واستبداله بمسار نسخ إحتياطي.

يقدم هذا المستند مثالا لكيفية إستخدام ميزة تعقب المسار الثابت على جهاز أمان PIX 500 Series أو جهاز الأمان القابل للتكيف ASA 5500 Series لتمكين الجهاز من إستخدام إتصالات الإنترنت المكررة أو الاحتياطية. في هذا المثال، يسمح تعقب المسار الثابت لجهاز الأمان باستخدام اتصال غير مكلف بموفر خدمة الإنترنت الثانوي (ISP) في حالة عدم توفر الخط المؤجر الأساسي.

لتحقيق هذا التكرار، يقوم جهاز الأمان بربط مسار ثابت بهدف مراقبة تقوم بتحديده. تقوم عملية إتفاقية مستوى الخدمة (SLA) بمراقبة الهدف باستخدام طلبات صدى بروتوكول رسائل التحكم في الإنترنت (ICMP) الدورية. إذا لم

يتم تلقي رد على صدى، يتم إعتبار الكائن معطلا، ويتم إزالة المسار المقترن من جدول التوجيه. يتم إستخدام مسار نسخ إحتياطي تم تكوينه مسبقا بدلا من المسار الذي تمت إزالته. أثناء إستخدام مسار النسخ الاحتياطي، تستمر عملية مراقبة SLA في محاولة الوصول إلى هدف المراقبة. وبمجرد توفر الهدف مرة أخرى، يتم إستبدال المسار الأول في جدول التوجيه، كما تتم إزالة مسار النسخ الاحتياطي.

ملاحظة: لا يمكن إستخدام التكوين الموضح في هذا المستند لموازنة الحمل أو مشاركة الحمل لأنه غير مدعوم على ASA/PIX . أستخدم هذا التكوين لأغراض التكرار أو النسخ الاحتياطي فقط. تستخدم حركة المرور الصادرة مزود خدمة الإنترنت (ISP) الأساسي ثم مزود خدمة الإنترنت (ISP) الثانوي، إذا فشل الأساسي. يتسبب فشل مزود خدمة الإنترنت (ISP) الأساسي في تعطيل حركة المرور بشكل مؤقت.

المتطلبات الأساسية

المتطلبات

أختر هدف مراقبة يمكنه الاستجابة لطلبات صدى ICMP. يمكن أن يكون الهدف أي كائن شبكة تختاره، ولكن من المستحسن وجود هدف مرتبط باتصال ISP الخاص بك بشكل وثيق. وتشمل بعض أهداف الرصد المحتملة ما يلي:

- عنوان بوابة ISP
- عنوان آخر تتم إدارته من ISP
- خادم على شبكة أخرى، مثل خادم AAA، يحتاج جهاز الأمان إلى الاتصال به
- لا يعد كائن الشبكة الدائم الموجود على شبكة أخرى (جهاز كمبيوتر مكتبي أو كمبيوتر محمول يمكنك إغلاقه ليلا خيارا جيدا)

يفترض هذا المستند أن جهاز الأمان قيد التشغيل الكامل وتم تكوينه للسماح ل Cisco ASDM بإجراء تغييرات التكوين.

ملاحظة: للحصول على معلومات حول كيفية السماح ل ASDM بتكوين الجهاز، ارجع إلى السماح بوصول HTTPS ل ASDM.

المكونات المستخدمة

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

- جهاز أمان Cisco PIX 515E مع إصدار البرنامج 7.2(1) أو إصدار أحدث
- Cisco Adaptive Security Device Manager 5.2(1) أو إصدار أحدث

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.

المنتجات ذات الصلة

يمكنك أيضا إستخدام هذا التكوين مع جهاز الأمان Cisco ASA 5500 Series Security Appliance، الإصدار 7.2(1).

ملاحظة: يلزم أمر **الواجهة الاحتياطية** لتكوين الواجهة الرابعة على ASA 5505. راجع واجهة النسخ الاحتياطي للحصول على مزيد من المعلومات.

الاصطلاحات

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

معلومات أساسية

في هذا المثال، يحتفظ جهاز الأمان باتصالين بالإنترنت. أول اتصال هو خط مؤجر عالي السرعة يتم الوصول إليه من خلال موجه يتم توفيره من قبل مزود خدمة الإنترنت (ISP) الرئيسي. بينما يمثل الاتصال الثاني خط مشترك رقمي أقل سرعة (DSL) يتم الوصول إليه من خلال مودم DSL يقدمه مزود خدمة الإنترنت (ISP) الثانوي.

ملاحظة: لا يحدث موازنة التحميل في هذا المثال.

يكون اتصال DSL خاملا طالما كان الخط المؤجر نشطا وكانت بوابة ISP الأساسية قابلة للوصول. ومع ذلك، في حالة انقطاع الاتصال ب ISP الأساسي، يقوم جهاز الأمان بتغيير جدول التوجيه إلى حركة مرور البيانات المباشرة إلى اتصال DSL. يتم إستخدام تعقب المسار الثابت للحصول على هذا التكرار.

تم تكوين جهاز الأمان باستخدام مسار ثابت يوجه جميع حركة مرور الإنترنت إلى ISP الأساسي. كل 10 ثوان تقوم عملية مراقبة SLA بالتحقق للتأكد من إمكانية الوصول إلى بوابة ISP الأساسية. إذا حددت عملية مراقبة SLA عدم إمكانية الوصول إلى بوابة ISP الأساسية، فسيتم إزالة المسار الثابت الذي يوجه حركة مرور البيانات إلى تلك الواجهة من جدول التوجيه. لاستبدال هذا المسار الثابت، يتم تثبيت مسار ثابت بديل يقوم بتوجيه حركة مرور البيانات إلى مزود خدمة الإنترنت (ISP) الثانوي. يوجه هذا المسار الثابت البديل حركة مرور البيانات إلى ISP الثانوي من خلال مودم DSL حتى يصبح الارتباط ب ISP الأساسي قابلا للوصول.

يوفر هذا التكوين طريقة غير مكلفة نسبيا لضمان بقاء الوصول إلى الإنترنت الصادر متاحا للمستخدمين خلف جهاز الأمان. كما هو موضح في هذا المستند، قد لا يكون هذا الإعداد مناسبا للوصول الوارد إلى الموارد الموجودة خلف جهاز الأمان. يلزم توفر مهارات شبكة متقدمة لتحقيق إتصالات داخلية تتسم بالسلاسة. لا يتم تغطية هذه المهارات في هذا المستند.

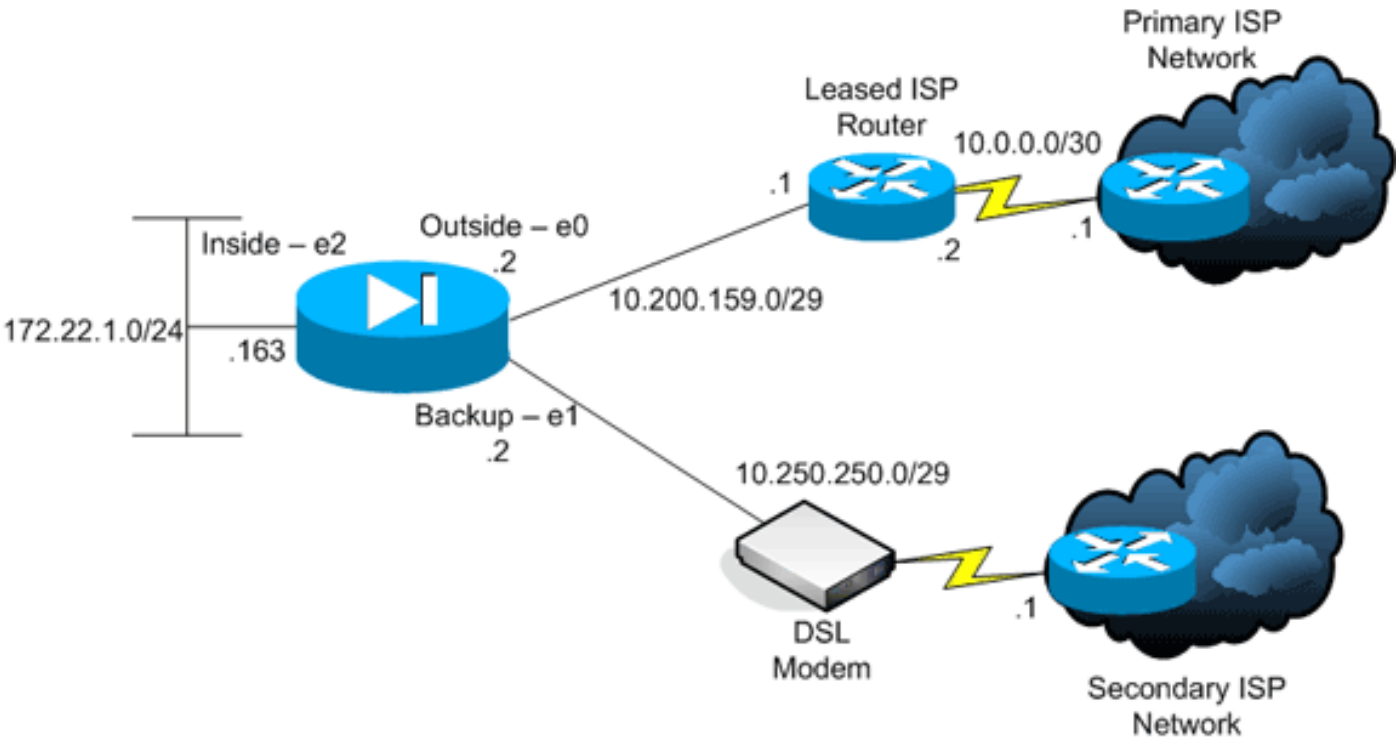
التكوين

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

ملاحظة: عناوين IP المستخدمة في هذا التكوين غير قابلة للتوجيه بشكل قانوني على الإنترنت. هم rfc 1918 عنوان أي يكون استعملت في مختبر بيئة.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



التكوينات

يستخدم هذا المستند التكوينات التالية:

- واجهة سطر الأوامر (CLI)
- مدير أجهزة حلول الأمان المعدلة (ASDM)

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

تكوين واجهة سطر الأوامر (CLI)

PIX

```
pix# show running-config
Saved :
:
(PIX Version 7.2(1
!
hostname pix
domain-name default.domain.invalid
enable password 9jNfZuG3TC5tCVH0 encrypted
names
!
interface Ethernet0
nameif outside
security-level 0
ip address 10.200.159.2 255.255.255.248
!
interface Ethernet1
nameif backup
The interface attached to the Secondary ISP. !--- ---!
"backup" was chosen here, but any name can be assigned.
security-level 0 ip address 10.250.250.2 255.255.255.248
! interface Ethernet2 nameif inside security-level 100
ip address 172.22.1.163 255.255.255.0 ! interface
```

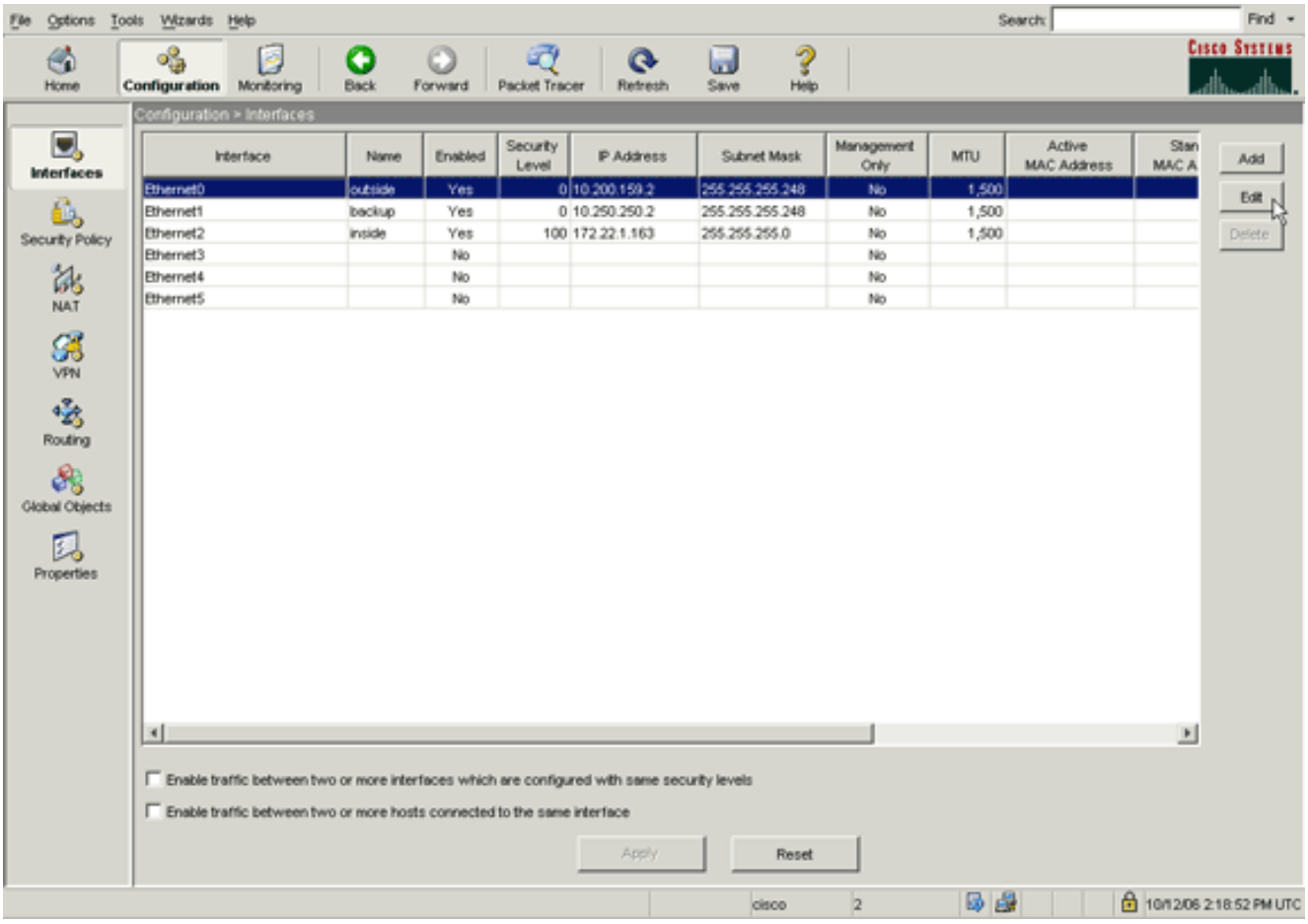
```
Ethernet3 shutdown no nameif no security-level no ip
address ! interface Ethernet4 shutdown no nameif no
security-level no ip address ! interface Ethernet5
shutdown no nameif no security-level no ip address !
passwd 2KFQnbNIdI.2KYOU encrypted ftp mode passive dns
server-group DefaultDNS domain-name
default.domain.invalid pager lines 24 logging enable
logging buffered debugging mtu outside 1500 mtu backup
1500 mtu inside 1500 no failover asdm image
flash:/asdm521.bin no asdm history enable arp timeout
14400 global (outside) 1 interface
global (backup) 1 interface
nat (inside) 1 172.16.1.0 255.255.255.0
NAT Configuration for Outside and Backup route ---!
outside 0.0.0.0 0.0.0.0 10.200.159.1 1 track 1
Enter this command in order to track a static ---!
route. !--- This is the static route to be installed in
the routing !--- table while the tracked object is
reachable. The value after !--- the keyword "track" is a
tracking ID you specify. route backup 0.0.0.0 0.0.0.0
10.250.250.1 254
Define the backup route to use when the tracked ---!
object is unavailable. !--- The administrative distance
of the backup route must be greater than !--- the
administrative distance of the tracked route. !--- If
the primary gateway is unreachable, that route is
removed !--- and the backup route is installed in the
routing table !--- instead of the tracked route. timeout
xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00
udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323
0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute
username cisco password ffIRPGpDSOJh9YLq encrypted http
server enable http 172.22.1.0 255.255.255.0 inside no
snmp-server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown
coldstart sla monitor 123
type echo protocol ipIcmpEcho 10.0.0.1 interface
outside
num-packets 3
frequency 10
Configure a new monitoring process with the ID 123. ---!
Specify the !--- monitoring protocol and the target
network object whose availability the tracking !---
process monitors. Specify the number of packets to be
sent with each poll. !--- Specify the rate at which the
monitor process repeats (in seconds). sla monitor
schedule 123 life forever start-time now
Schedule the monitoring process. In this case the ---!
lifetime !--- of the process is specified to be forever.
The process is scheduled to begin !--- at the time this
command is entered. As configured, this command allows
the !--- monitoring configuration specified above to
determine how often the testing !--- occurs. However,
you can schedule this monitoring process to begin in the
!--- future and to only occur at specified times. !
track 1 rtr 123 reachability
Associate a tracked static route with the SLA ---!
monitoring process. !--- The track ID corresponds to the
track ID given to the static route to monitor: !---
route outside 0.0.0.0 0.0.0.0 10.0.0.2 1 track 1 !---
"rtr" = Response Time Reporter entry. 123 is the ID of
.the SLA process !--- defined above
```

```
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:a4a0e9be4593ad43bc17a1cc25e32dc2
end :
```

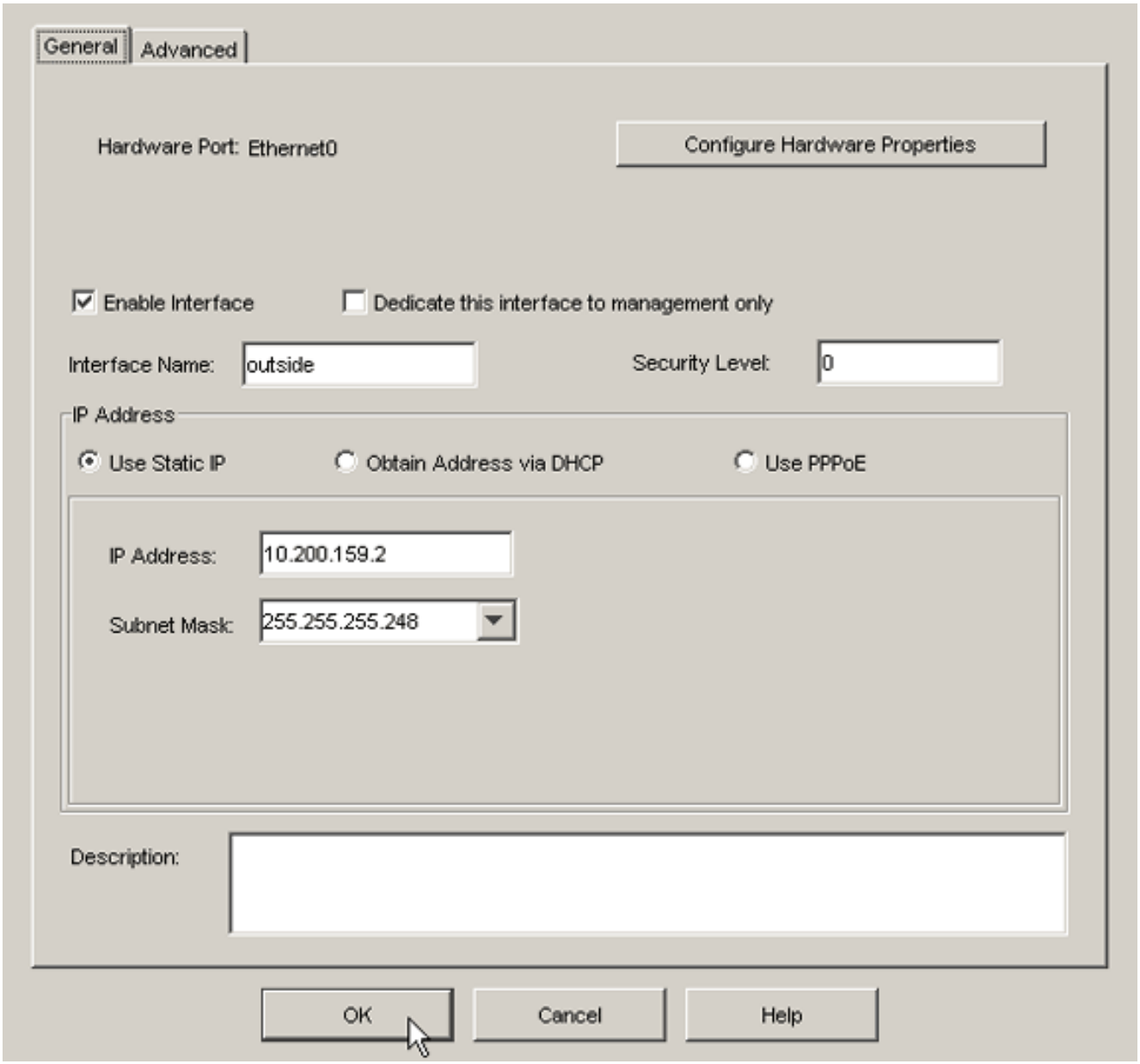
تكوين ASDM

لتكوين دعم ISP الاحتياطي أو الاحتياطي باستخدام تطبيق ASDM، أكمل الخطوات التالية:

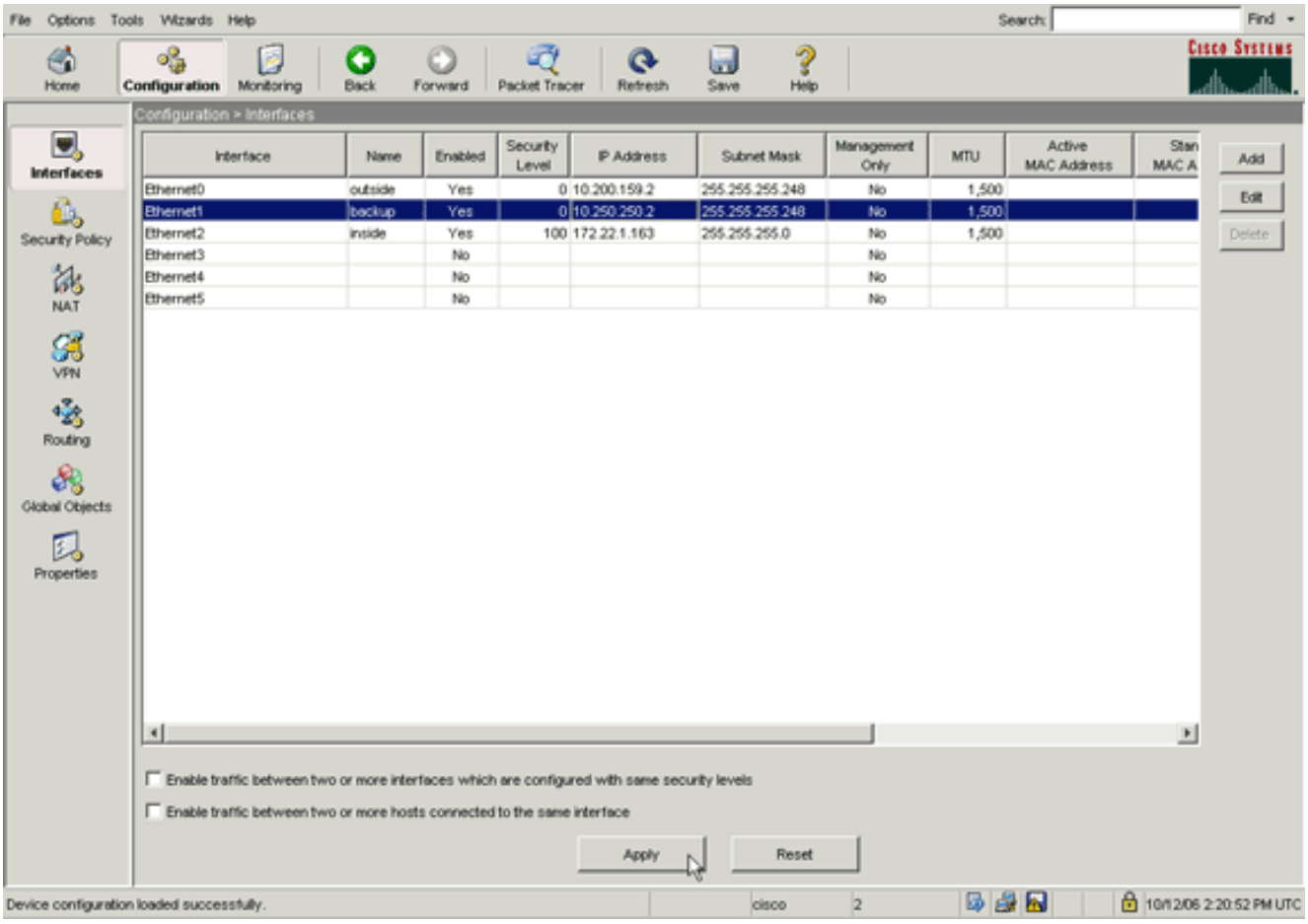
1. في تطبيق ASDM، انقر فوق **تكوين**، ثم انقر فوق **الواجهات**.



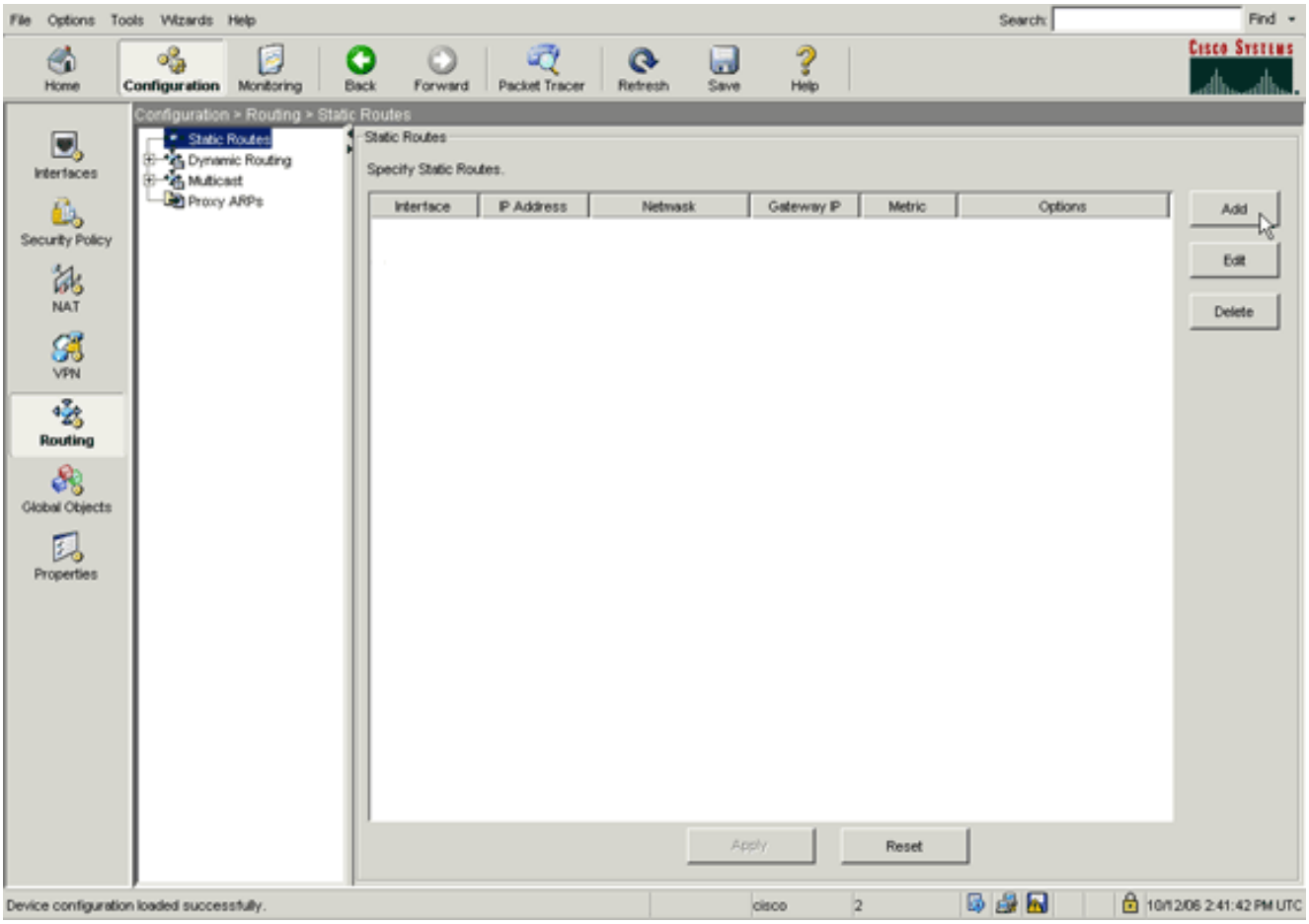
2. من قائمة الواجهات، حدد **Ethernet0**، ثم انقر **تحرير**.يظهر مربع الحوار هذا.



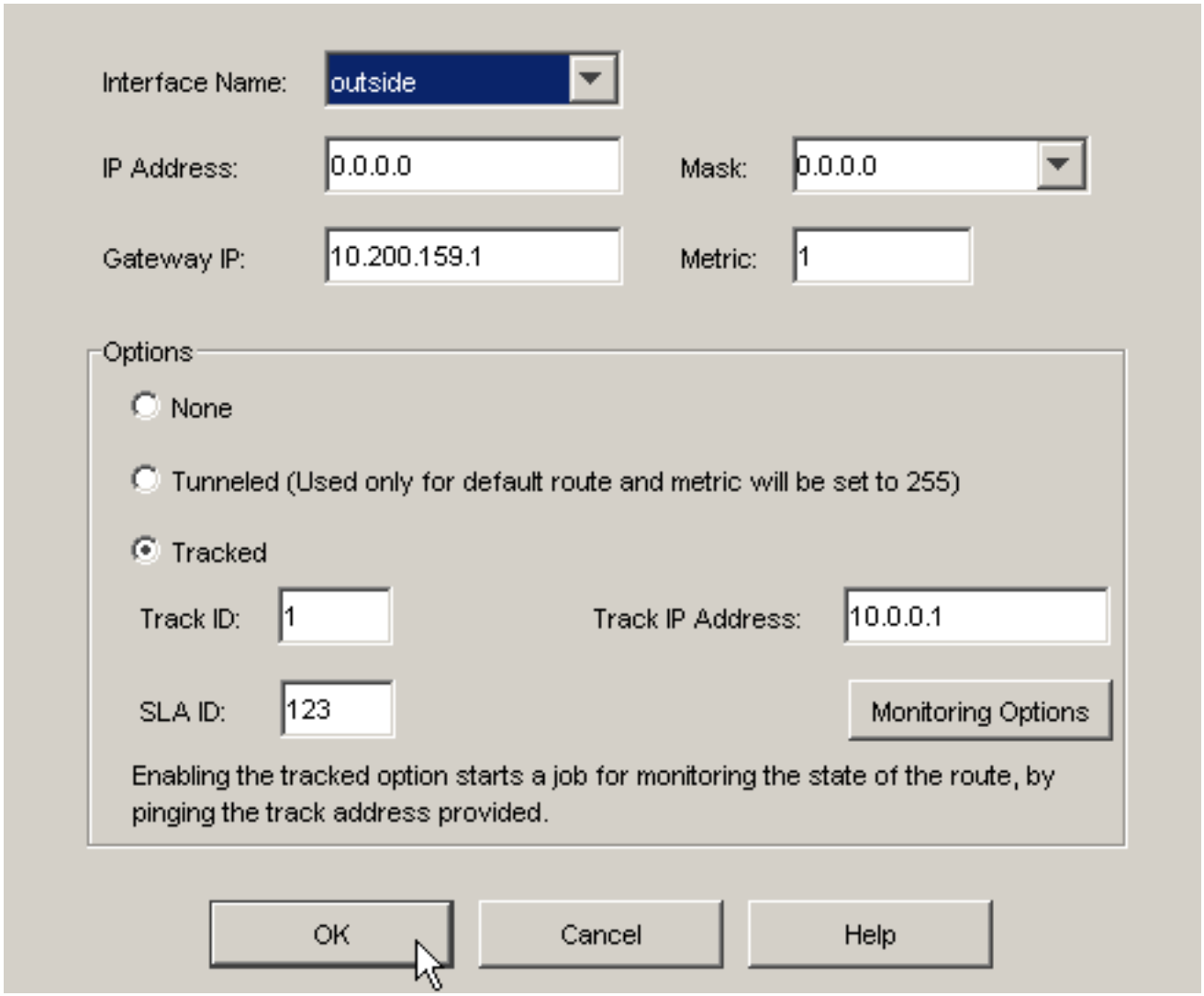
3. حدد خانة الاختيار **تمكين الواجهة**، وأدخل قيم في حقول اسم الواجهة ومستوى الأمان وعنوان IP وقناع الشبكة الفرعية.
4. طقطقة ok in order to أغلقت الشاشة.
5. قم بتكوين الواجهات الأخرى حسب الحاجة، وانقر فوق **تطبيق** لتحديث تكوين جهاز الأمان.



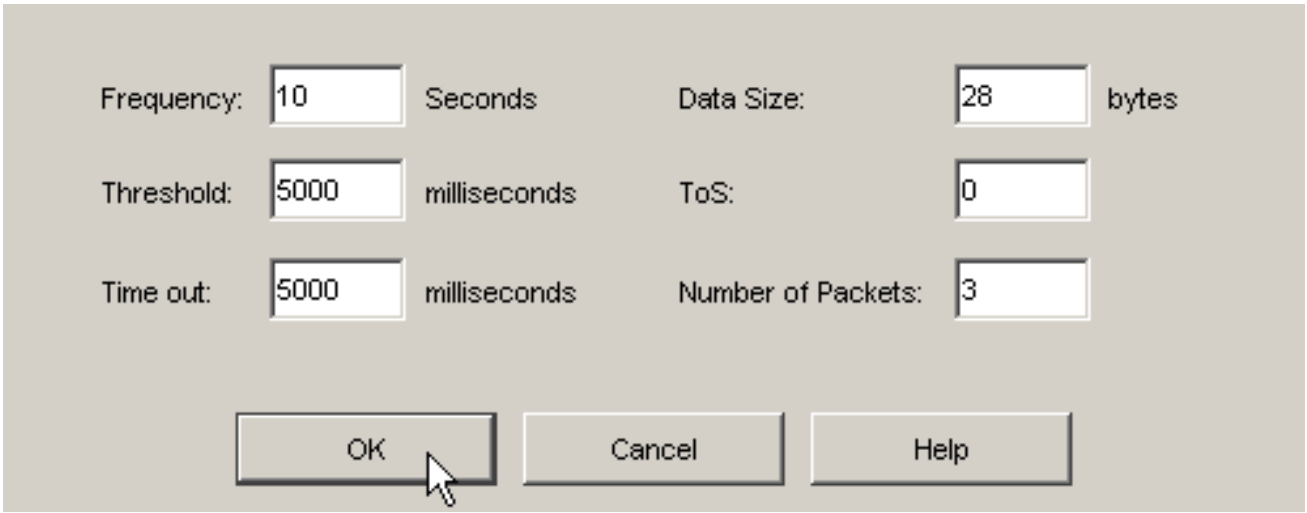
6. انقر فوق **التوجيه** الموجود على الجانب الأيسر من تطبيق ASDM.



7. انقر فوق **إضافة** لإضافة المسارات الثابتة الجديدة.يظهر مربع الحوار هذا.



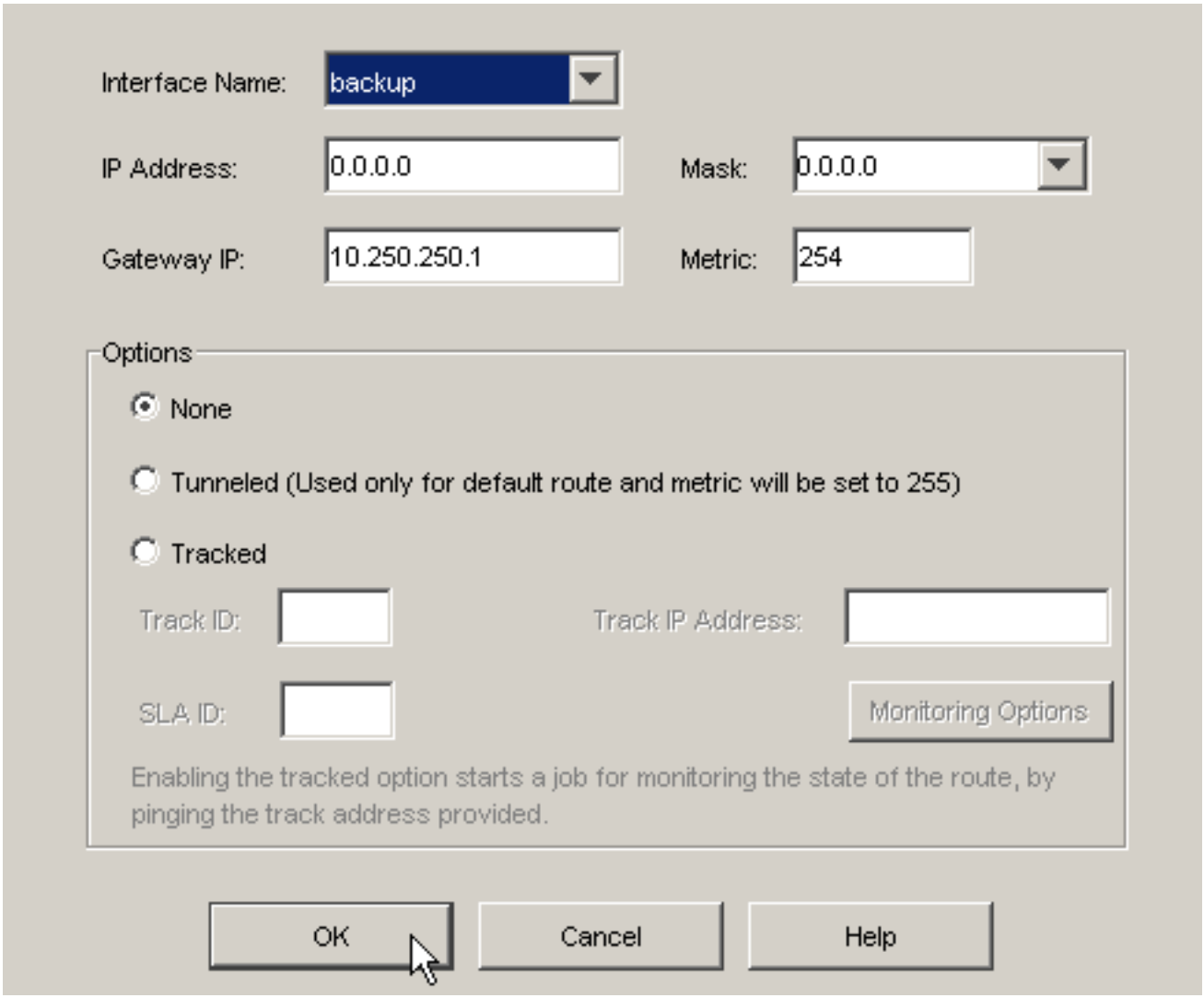
8. من القائمة المنسدلة اسم الواجهة، أختر الواجهة التي يتواجد عليها المسار، وقم بتكوين المسار الافتراضي للوصول إلى البوابة. في هذا المثال، يمثل الإصدار 10.0.0.1 بوابة ISP الأساسية، بالإضافة إلى الكائن الذي تريد مراقبته باستخدام أصداء ICMP.
9. في منطقة "الخيارات"، انقر زر **الاختيار** المتتبع، وأدخل قيم في حقول معرف المسار، ومعرف SLA، وعنوان المسار.
10. انقر فوق **خيارات المراقبة**.يظهر مربع الحوار هذا.



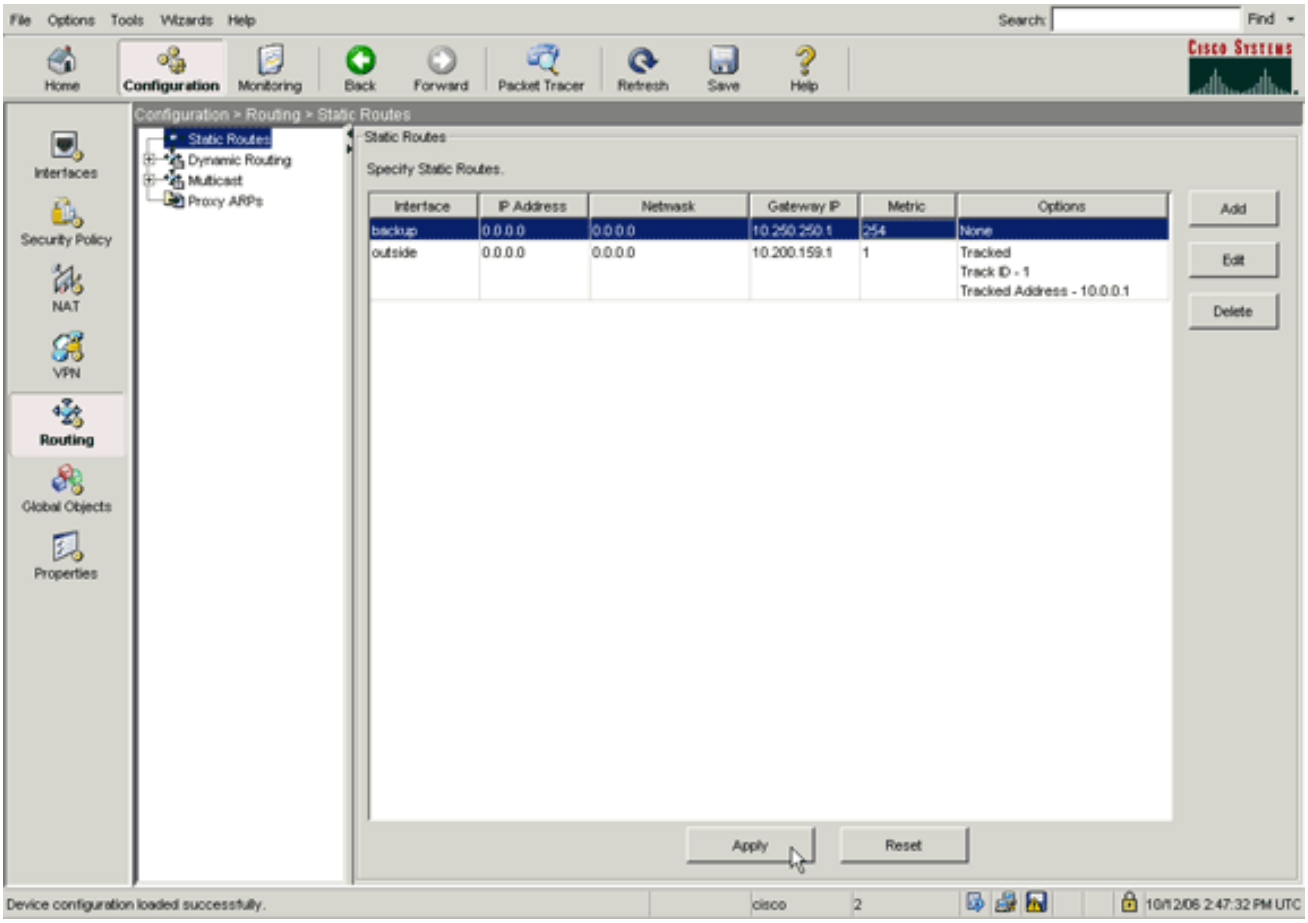
11. قم بإدخال قيم للتردد وخيارات المراقبة الأخرى، وانقر **موافق**.
12. قم بإضافة مسار ثابت آخر ل ISP الثانوي من أجل توفير مسار للوصول إلى الإنترنت.ولجعله مسارا ثانويا، قم بتكوين هذا المسار باستخدام مقياس أعلى، مثل 254. في حالة فشل المسار الرئيسي (ISP الأساسي)، تتم

إزالة هذا المسار من جدول التوجيه. يتم تثبيت هذا المسار الثانوي (ISP الثانوي) في جدول توجيه PIX بدلا من ذلك.

13. طقطقة **ok** in order to أغلقت الشاشة.



تظهر التكوينات في قائمة الواجهة.



14. حدد تكوين التوجيه، وانقر فوق **تطبيق** لتحديث تكوين جهاز الأمان.

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تأكيد اكتمال التكوين

أستخدم أوامر **العرض** هذه للتحقق من اكتمال التكوين الخاص بك.

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

- **show running-config sla monitor**— يعرض أوامر SLA في التكوين.

```
pix# show running-config sla monitor
sla monitor 123
type echo protocol ipIcmpEcho 10.0.0.1 interface outside
num-packets 3
frequency 10
sla monitor schedule 123 life forever start-time now
```

- **show sla monitor configuration** — يعرض إعدادات التكوين الحالية للعملية.

```
pix# show sla monitor configuration 123
.IP SLA Monitor, Infrastructure Engine-II
Entry number: 123
:Owner
:Tag
Type of operation to perform: echo
Target address: 10.0.0.1
Interface: outside
```

```
                                Number of packets: 3
                      Request size (ARR data portion): 28
                  Operation timeout (milliseconds): 5000
                         Type Of Service parameters: 0x0
                                  Verify data: No
                  Operation frequency (seconds): 10
Next Scheduled Start Time: Start Time already passed
                                Group Scheduled : FALSE
                                Life (seconds): Forever
                             Entry Ageout (seconds): never
                      Recurring (Starting Everyday): FALSE
                  Status of entry (SNMP RowStatus): Active
                                :Enhanced History
```

- **show sla monitor operation-state**—يعرض الإحصائيات التشغيلية لعملية SLA.قبل فشل مزود خدمة الإنترنت (ISP) الأساسي، تكون هذه هي حالة التشغيل:

```
pix# show sla monitor operational-state 123
                                Entry number: 123
            Modification time: 13:59:37.824 UTC Thu Oct 12 2006
                Number of Octets Used by this Entry: 1480
                    Number of operations attempted: 367
                        Number of operations skipped: 0
                Current seconds left in Life: Forever
                   Operational state of entry: Active
                Last time this entry was reset: Never
                        Connection loss occurred: FALSE
                                Timeout occurred: FALSE
                            Over thresholds occurred: FALSE
                              Latest RTT (milliseconds): 1
        Latest operation start time: 15:00:37.825 UTC Thu Oct 12 2006
                              Latest operation return code: OK
                                        :RTT Values
             RTTAvg: 1        RTTMin: 1        RTTMax: 1
            NumOfRTT: 3      RTTSum: 3        RTTSum2: 3
```

بعد فشل مزود خدمة الإنترنت (ISP) الأساسي (وإجازة مهلة بروتوكول ICMP للإصداء)، تكون هذه هي حالة التشغيل:

```
pix# show sla monitor operational-state
                                Entry number: 123
            Modification time: 13:59:37.825 UTC Thu Oct 12 2006
                Number of Octets Used by this Entry: 1480
                    Number of operations attempted: 385
                        Number of operations skipped: 0
                Current seconds left in Life: Forever
                   Operational state of entry: Active
                Last time this entry was reset: Never
                        Connection loss occurred: FALSE
                                Timeout occurred: TRUE
                            Over thresholds occurred: FALSE
                Latest RTT (milliseconds): NoConnection/Busy/Timeout
        Latest operation start time: 15:03:27.825 UTC Thu Oct 12 2006
                              Latest operation return code: Timeout
                                        :RTT Values
             RTTAvg: 0        RTTMin: 0        RTTMax: 0
            NumOfRTT: 0      RTTSum: 0        RTTSum2: 0
```

تأكيد تثبيت مسار النسخ الاحتياطي (أسلوب واجهة سطر الأوامر)

أستخدم الأمر **show route** لتحديد وقت تثبيت مسار النسخ الاحتياطي.

- قبل فشل ISP الأساسي، هذا هو جدول التوجيه:

```
pix# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       candidate default, U - per-user static route, o - ODR - *
                           P - periodic downloaded static route

                  Gateway of last resort is 10.200.159.1 to network 0.0.0.0

                     S    64.101.0.0 255.255.0.0 [1/0] via 172.22.1.1, inside
                  C    172.22.1.0 255.255.255.0 is directly connected, inside
                   C    10.250.250.0 255.255.255.248 is directly connected, backup
                  C    10.200.159.0 255.255.255.248 is directly connected, outside
                        S*   0.0.0.0 0.0.0.0 [1/0] via 10.200.159.1, outside
```

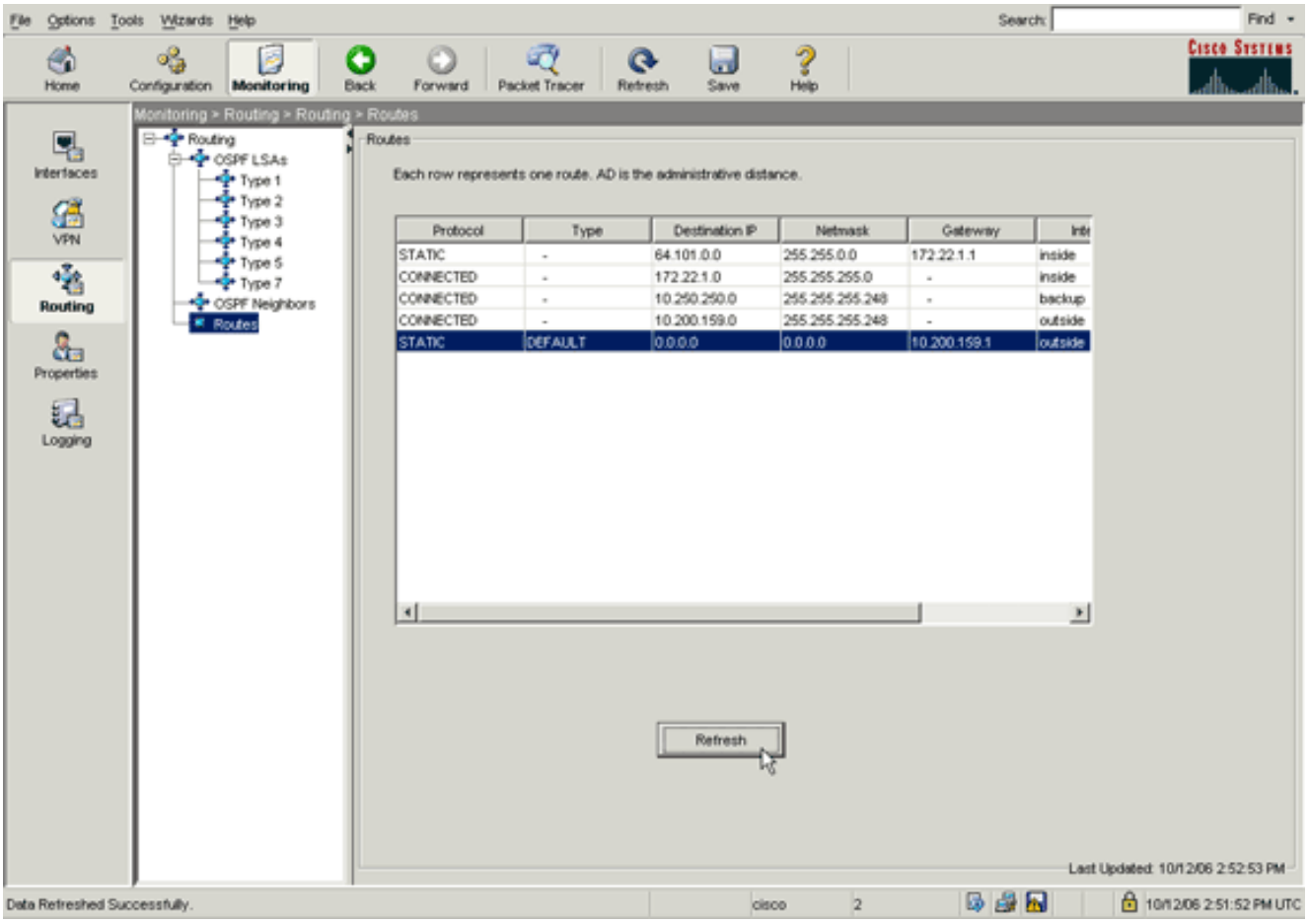
بعد فشل مزود خدمة الإنترنت (ISP) الأساسي، تتم إزالة المسار الثابت، ويتم تثبيت مسار النسخ الاحتياطي، وهذا هو جدول التوجيه:

```
pix(config)# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       candidate default, U - per-user static route, o - ODR - *
                           P - periodic downloaded static route

                  Gateway of last resort is 10.250.250.1 to network 0.0.0.0

                     S    64.101.0.0 255.255.0.0 [1/0] via 172.22.1.1, inside
                  C    172.22.1.0 255.255.255.0 is directly connected, inside
                   C    10.250.250.0 255.255.255.248 is directly connected, backup
                  C    10.200.159.0 255.255.255.248 is directly connected, outside
                        S*   0.0.0.0 0.0.0.0 [254/0] via 10.250.250.1, backup
```

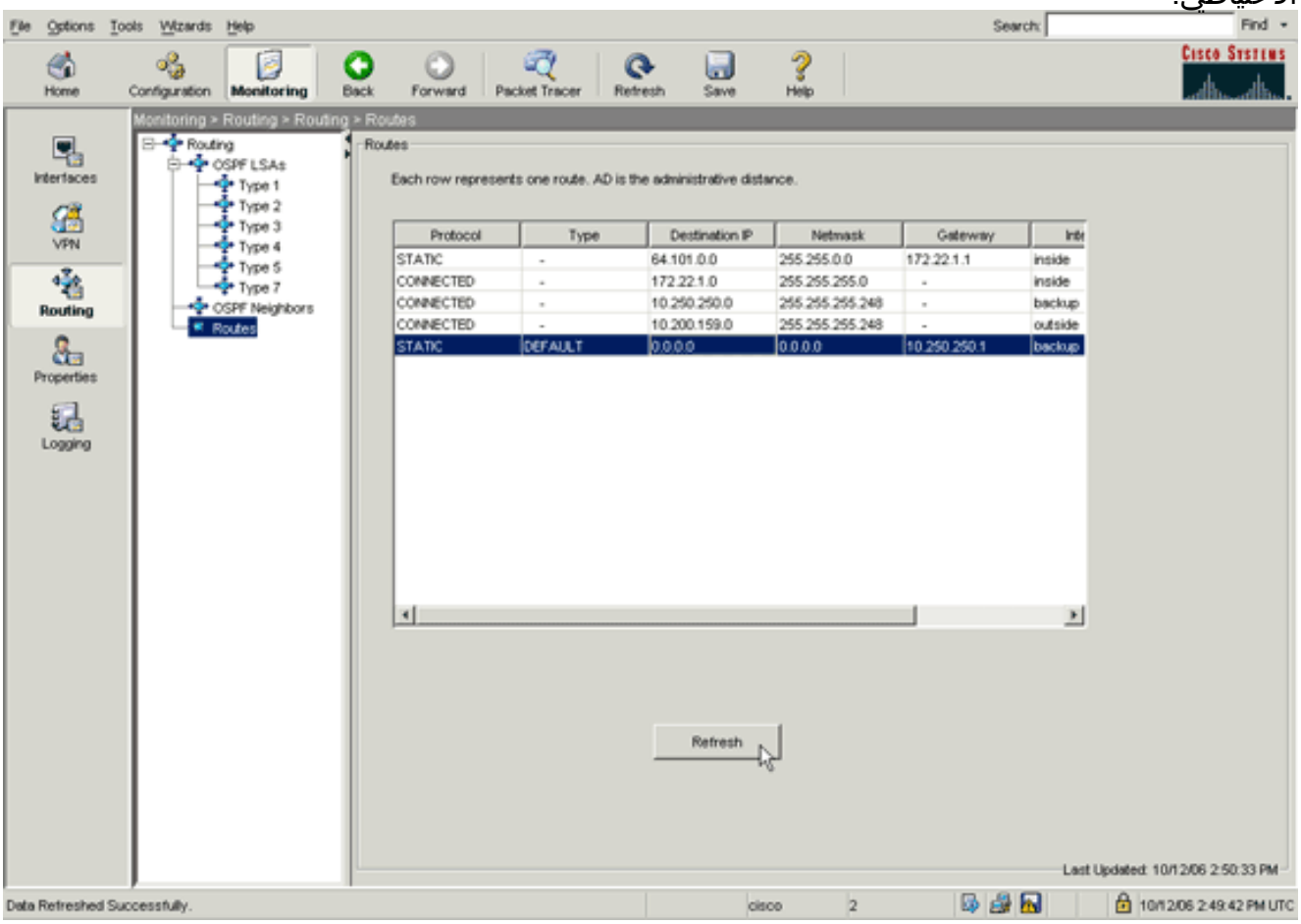
تأكيد تثبيت مسار النسخ الاحتياطي (أسلوب ASDM)

للتأكد مع ASDM أن مسار النسخ الاحتياطي مثبت، أكمل الخطوات التالية:

1. انقر فوق **المراقبة**، ثم انقر فوق **التوجيه**.
2. من شجرة التوجيه، أختر **المسارات**.قبل فشل ISP الأساسي، هذا هو جدول التوجيه:



يشير المسار الافتراضي إلى 10.0.0.2 من خلال الواجهة الخارجية.وبعد فشل مزود خدمة الإنترنت (ISP) الأساسي، تتم إزالة المسار، ويتم تثبيت مسار النسخ الاحتياطي. يشير المسار الافتراضي الآن إلى 10.250.250.1 من خلال واجهة النسخ الاحتياطي.



استكشاف الأخطاء وإصلاحها

أوامر التصحيح

- **debug sla monitor trace**—يعرض تقدم عملية echo.تم تشغيل الكائن الذي تم تتبعه (بوابة ISP الأساسية)، ونجح صدى ICMP.

```
IP SLA Monitor(123) Scheduler: Starting an operation
IP SLA Monitor(123) echo operation: Sending an echo operation
IP SLA Monitor(123) echo operation: RTT=3 OK
IP SLA Monitor(123) echo operation: RTT=3 OK
IP SLA Monitor(123) echo operation: RTT=4 OK
IP SLA Monitor(123) Scheduler: Updating result
```

تم إيقاف الكائن الذي تم تتبعه (بوابة ISP الأساسية)، وتفشل أصداء ICMP.

```
IP SLA Monitor(123) Scheduler: Starting an operation
IP SLA Monitor(123) echo operation: Sending an echo operation
IP SLA Monitor(123) echo operation: Timeout
IP SLA Monitor(123) echo operation: Timeout
IP SLA Monitor(123) echo operation: Timeout
IP SLA Monitor(123) Scheduler: Updating result
```

- **debug sla monitor error**—يعرض الأخطاء التي تواجهها مراقبة SLA.تم تشغيل الكائن المتتبع (بوابة ISP الأساسية)، ونجح ICMP.

```
PIX-7-609001: Built local-host NP Identity Ifc:10.200.159.2%
PIX-7-609001: Built local-host outside:10.0.0.1%
PIX-6-302020: Built ICMP connection for faddr 10.0.0.1/0 gaddr%
laddr 10.200.159.2/52696 10.200.159.2/52696
PIX-6-302021: Teardown ICMP connection for faddr 10.0.0.1/0 gaddr%
laddr 10.200.159.2/52696 10.200.159.2/52696
PIX-7-609002: Teardown local-host NP Identity Ifc:10.200.159.2 duration%
0:00:00
PIX-7-609002: Teardown local-host outside:10.0.0.1 duration 0:00:00%
PIX-7-609001: Built local-host NP Identity Ifc:10.200.159.2%
PIX-7-609001: Built local-host outside:10.0.0.1%
PIX-6-302020: Built ICMP connection for faddr 10.0.0.1/0 gaddr%
laddr 10.200.159.2/52697 0.200.159.2/52697
PIX-6-302021: Teardown ICMP connection for faddr 10.0.0.1/0 gaddr%
laddr 10.200.159.2/52697 10.200.159.2/52697
PIX-7-609002: Teardown local-host NP Identity Ifc:10.200.159.2%
duration 0:00:00
PIX-7-609002: Teardown local-host outside:10.0.0.1 duration 0:00:00%
```

تم إيقاف الكائن الذي تم تعقبه (بوابة ISP الأساسية)، وتمت إزالة المسار الذي تم تعقبه.

```
PIX-7-609001: Built local-host NP Identity Ifc:10.200.159.2%
PIX-7-609001: Built local-host outside:10.0.0.1%
PIX-6-302020: Built ICMP connection for faddr 10.0.0.1/0 gaddr%
laddr 10.200.159.2/6405 10.200.159.2/6405
PIX-6-302020: Built ICMP connection for faddr 10.0.0.1/0 gaddr%
laddr 10.200.159.2/6406 10.200.159.2/6406
PIX-6-302020: Built ICMP connection for faddr 10.0.0.1/0 gaddr%
laddr 10.200.159.2/6407 10.200.159.2/6407
PIX-6-302021: Teardown ICMP connection for faddr 10.0.0.1/0 gaddr%
laddr 10.200.159.2/6405 10.200.159.2/6405
PIX-6-302021: Teardown ICMP connection for faddr 10.0.0.1/0 gaddr%
laddr 10.200.159.2/6406 10.200.159.2/6406
PIX-6-302021: Teardown ICMP connection for faddr 10.0.0.1/0 gaddr%
laddr 10.200.159.2/6407 10.200.159.2/6407
PIX-7-609002: Teardown local-host NP Identity Ifc:10.200.159.2%
duration 0:00:02
PIX-7-609002: Teardown local-host outside:10.0.0.1 duration 0:00:02%
,PIX-6-622001: Removing tracked route 0.0.0.0 0.0.0.0 10.200.159.1%
distance 1, table Default-IP-Routing-Table, on interface
```

```
outside
.is unreachable, so the route to the Primary ISP is removed 10.0.0.1 ---!
```

تمت إزالة المسار المتتبع بشكل غير ضروري

إذا تمت إزالة المسار المتتبع بشكل غير ضروري، فتأكد من أن هدف المراقبة الخاص بك متوفر دائما لتلقي طلبات الارتداد. بالإضافة إلى ذلك، تأكد من أن حالة هدف المراقبة (أي ما إذا كان الهدف يمكن الوصول إليه أم لا) مرتبطة إرتباطا وثيقا بحالة اتصال ISP الأساسي.

إذا قمت باختيار هدف مراقبة أبعد من بوابة ISP، فقد يفشل إرتباط آخر على هذا المسار أو قد يتداخل جهاز آخر. قد يتسبب هذا التكوين في قيام مراقبة SLA باستنتاج فشل الاتصال ب ISP الأساسي وتسبب في فشل جهاز الأمان بشكل غير ضروري إلى إرتباط ISP الثانوي.

على سبيل المثال، إذا قمت باختيار موجه مكتب فرعي كهدف للمراقبة، فقد يفشل اتصال ISP بالمكتب الفرعي، فضلا عن أي إرتباط آخر على طول الطريق. بمجرد فشل صدى ICMP الذي يتم إرساله بواسطة عملية المراقبة، يتم إزالة المسار الرئيسي المتتبع، حتى ولو كان إرتباط ISP الأساسي لا يزال نشطا.

في هذا المثال، تتم إدارة بوابة ISP الأساسية التي يتم إستخدامها كهدف مراقبة بواسطة ISP وتقع على الجانب الآخر من إرتباط ISP. يضمن هذا التكوين أنه في حالة فشل أصداء ICMP التي يتم إرسالها بواسطة عملية المراقبة، يكون إرتباط ISP معطلا بالتأكيد تقريبا.

مراقبة SLA على ASA

المشكلة:

لا تعمل مراقبة SLA بعد ترقية ASA إلى الإصدار 8.0.

الحل:

قد تكون المشكلة ناجمة عن الأمر **ip reverse-path** الذي تم تكوينه في الواجهة **الخارجية**. قم بإزالة الأمر في ASA وحاول التحقق من مراقبة SLA.

معلومات ذات صلة

- تكوين تعقب المسار الثابت
- مرجع أوامر PIX/ASA 7.2
- أجهزة الأمان Cisco ASA 5500 Series Security Appliances
- أجهزة الأمان Cisco PIX 500 Series Security Appliances
- 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).