ASA/PIX 7.x： 冗長またはバックアップ ISP リンクの設定例

目次

はじめに

スタティック ルートには、ルートがアップ状態かダウン状態かを判別するためのメカニズムが備わっていないという問題があります。 ネクストホップ ゲートウェイが使用不能になっても、ルートはルーティング テーブルに存在し続けます。 スタティック ルートがルーティング テーブルから削除されるのは、セキュリティ アプライアンス上の関連付けられているインターフェイスがダウンした場合だけです。 この問題を解決するために、スタティック ルート トラッキング機能を使用してスタティック ルートが使用可能かどうかをトラッキングし、ルートに障害が発生した場合はそのルートをルーティング テーブルから削除してバックアップ ルートに置き換えます。

このドキュメントでは、PIX 500 シリーズ セキュリティ アプライアンスまたは ASA 5500 シリーズ適応型セキュリティ アプライアンスでスタティック ルート トラッキングを使用して冗長インターネット接続またはバックアップ インターネット接続を有効にする方法の例を紹介します。 この例では、スタティック ルート トラッキングを使用することで、プライマリ専用回線が使用不能になった場合でも、セキュリティ アプライアンスからセカンダリ インターネット サービス プロ

バイダー（ISP）へ安価な接続を使用できるようにします。

この冗長性を実現するために、セキュリティ アプライアンスでモニタリング ターゲットと定義済みのスタティック ルートとを関連付けます。 サービス レベル契約（SLA）動作が定期的にインターネット制御メッセージ プロトコル（ICMP）エコー要求を送信してターゲットをモニタします。 エコー応答がない場合は、そのオブジェクトはダウンしていると見なされ、関連付けられているルートがルーティング テーブルから削除されます。 そして、削除されたルートに代わって、すでに定義されているバックアップ ルートが使用されます。 バックアップ ルートが使用されている間も、SLA モニタ動作はモニタリング ターゲットへの到達を試行し続けます。 再度、ターゲットに到達できるようになると、最初のルートがルーティング テーブルに置き換えられ、バックアップ ルートは削除されます。

注: ASA/PIX ではロード バランシングまたはロード シェアリングをサポートしていないため、このドキュメントで説明する設定をこの目的に使用することはできません。 この設定は冗長化またはバックアップの用途にだけ使用してください。 発信トラフィックはプライマリ ISP を使用し、プライマリ ISP に障害が発生した場合はセカンダリ ISP を使用します。 プライマリ ISP に障害が発生すると、一時的にトラフィックが中断されます。

前提条件

要件

ICMP エコー要求に応答できるモニタリング ターゲットを選択します。 任意のネットワーク オブジェクトをターゲットとして選択できますが、ISP 接続と緊密に結びついているオブジェクトをターゲットにすることを推奨します。 モニタリング ターゲットにできるオブジェクトの例を示します。

- ISP ゲートウェイ アドレス
- 別の ISP-managed アドレス
- 別のネットワーク上にあり、セキュリティ アプライアンスが通信する必要のある サーバ（AAA サーバなど）
- 別のネットワーク上で常時稼働している永続ネットワーク オブジェクト（夜間にシャットダウンされる可能性があるデスクトップ コンピュータやノートパソコンは推奨しません）

このドキュメントでは、セキュリティ アプライアンスが完全に動作していて、Cisco ASDM で設定を変更できるように設定されていることを前提としています。

注: デバイスの設定を ASDM で変更できるようにする方法については、『ASDM 用の HTTPS アクセスの許可』を参照してください。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- ソフトウェア バージョン 7.2(1) 以降がインストールされた Cisco PIX セキュリティ アプライアンス 515E
- Cisco Adaptive Security Device Manager 5.2(1) 以降

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

関連製品

この設定は、Cisco ASA 5500 シリーズ セキュリティ アプライアンス 7.2(1) 以降でも使用できます。

注: ASA 5505 の 4 つ目のインターフェイスの設定には **backup interface** コマンドが必要になります。 詳細については「backup interface」を参照してください。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

この例では、セキュリティ アプライアンスからインターネットへの接続を 2 つ保持しています。1 つ目の接続は高速専用回線です。この回線には、プライマリ ISP のルータを経由してアクセスします。 2 つ目の接続は低速デジタル加入者線（DSL）です。この回線には、セカンダリ ISP の DSL モデムを経由してアクセスします。

注: この例ではロード バランシングは行われません。

専用回線がアクティブでプライマリ ISP ゲートウェイが到達可能である限り、DSL 接続はアイドル状態となります。 ただし、プライマリ ISP への接続がダウンすると、セキュリティ アプライアンスのルーティング テーブルが変更され、トラフィックは DSL 接続に転送されるようになります。 スタティック ルート トラッキングは、こうした冗長性を実現するために使用されます。

セキュリティ アプライアンスの設定には、すべてのインターネット トラフィックをプライマリ ISP に転送するスタティック ルートを使用します。 プライマリ ISP ゲートウェイが到達可能かどうかは、SLA モニタ プロセスを使用して 10 秒間隔で確認します。 プライマリ ISP ゲートウェイに到達不能であると SLA モニタ プロセスが判定すると、そのインターフェイスにトラフィックを転送するスタティック ルートはルーティング テーブルから削除されます。 このスタティック ルートを置き換えるために、セカンダリ ISP にトラフィックを転送する代替スタティック ルートがインストールされます。 この代替スタティック ルートは、プライマリ ISP へのリンクが到達可能になるまで、DSL モデム経由でセカンダリ ISP にトラフィックを転送します。

この設定を使用すると、セキュリティ アプライアンスの背後にいるユーザがインターネットに発信アクセスができる状態を比較的安価に維持できます。 このドキュメントで説明したとおり、この設定は、セキュリティ アプライアンスの背後にあるリソースへの着信アクセスには適していない可能性があります。 シームレスな着信接続を実現するには、高度なネットワーキング スキルが必要です。 そうしたスキルについては、このドキュメントでは説明していません。

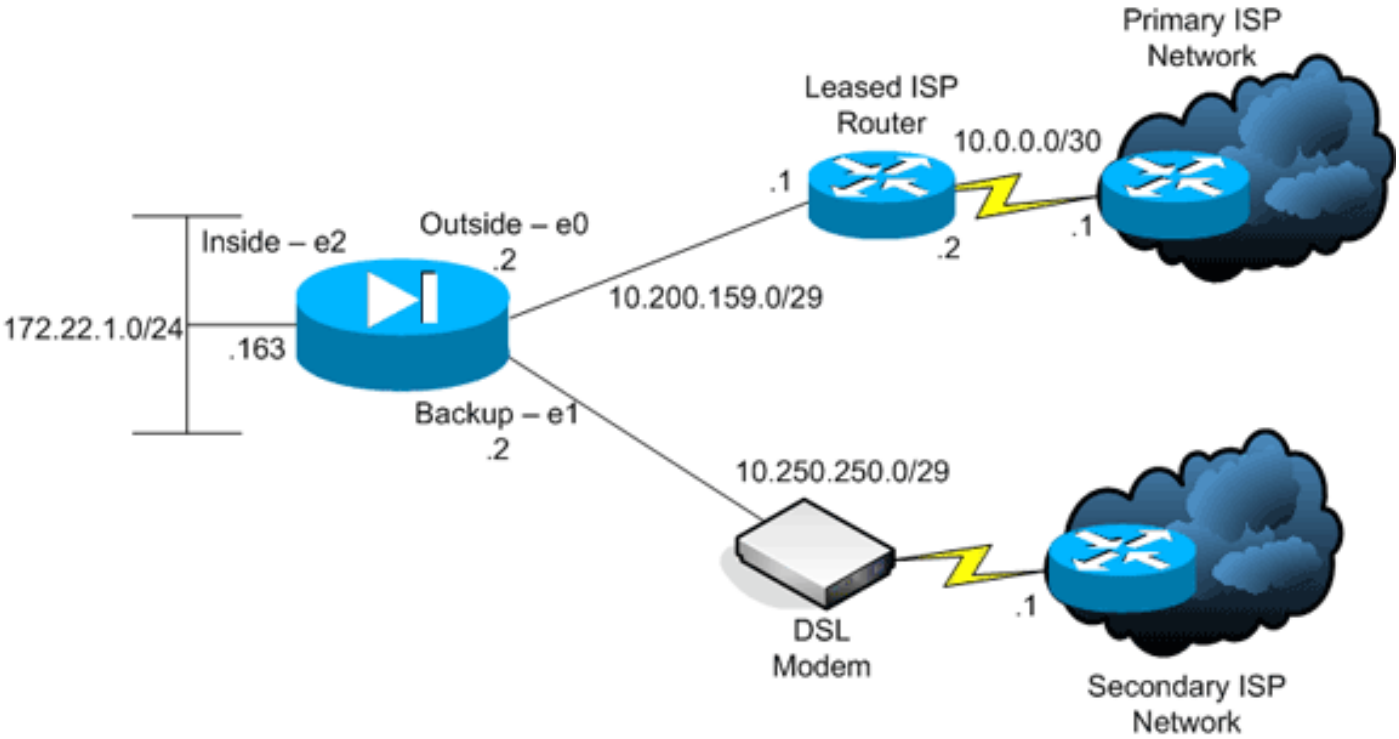
設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: この設定で使用している IP アドレスは、インターネット上で正式にルーティング可能なものではありません。 これらは RFC 1918 でのアドレスであり、ラボ環境で使用されているものです。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



設定

このドキュメントでは、次の設定を使用します。

- コマンドライン インターフェイス（CLI）
- Adaptive Security Device Manager（ASDM）

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

CLI 設定

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.
```

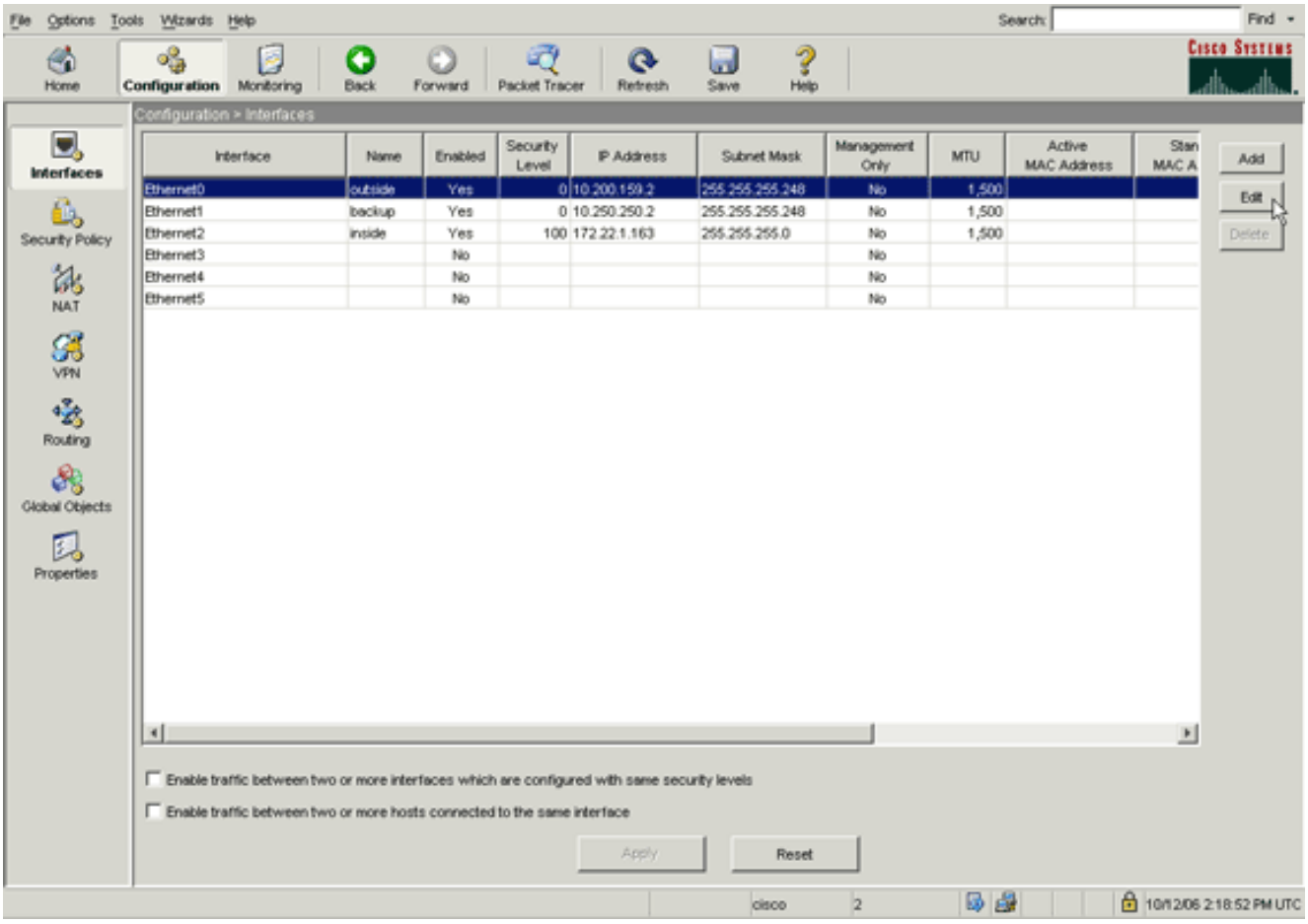
```
security-level 0 ip address 10.250.250.2 255.255.255.248
! interface Ethernet2 nameif inside security-level 100
ip address 172.22.1.163 255.255.255.0 ! interface
Ethernet3 shutdown no nameif no security-level no ip
address ! interface Ethernet4 shutdown no nameif no
security-level no ip address ! 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
```

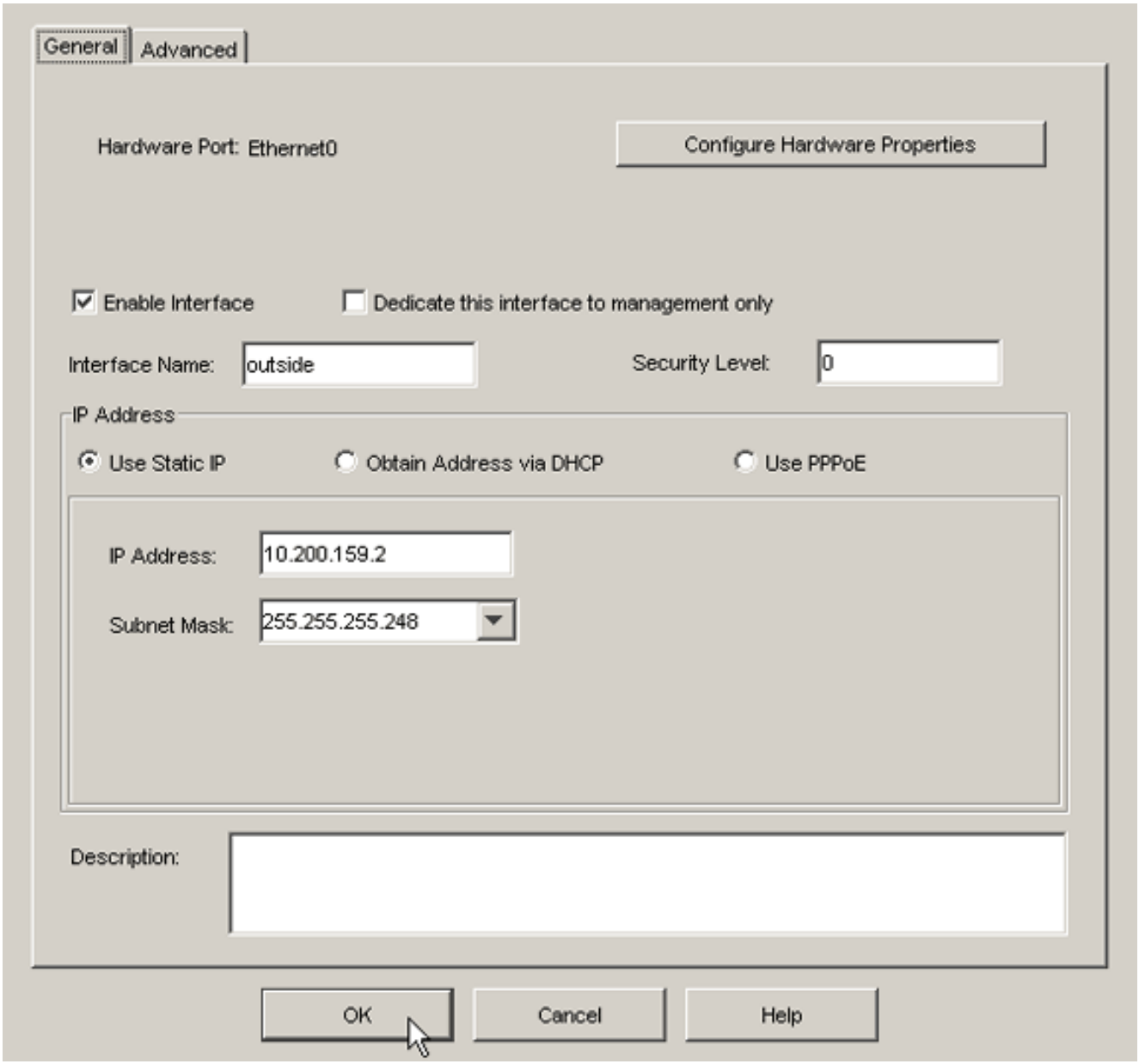
ASDM の設定

ASDM アプリケーションを使用して冗長 ISP サポートまたはバックアップ ISP サポートを設定するには、次の手順を実行します。

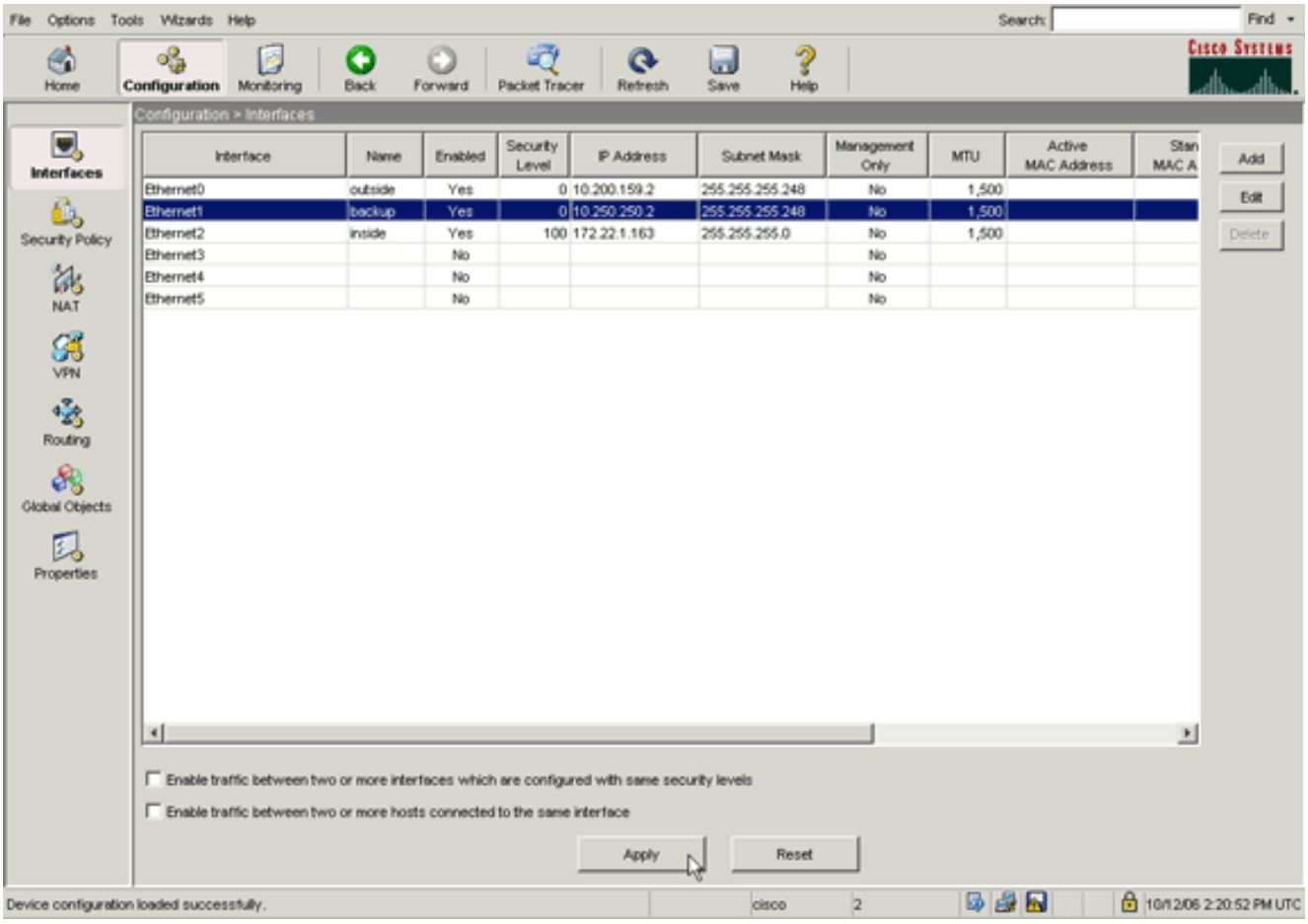
1. ASDM アプリケーションで [Configuration] をクリックし、続いて [Interfaces] をクリックします。



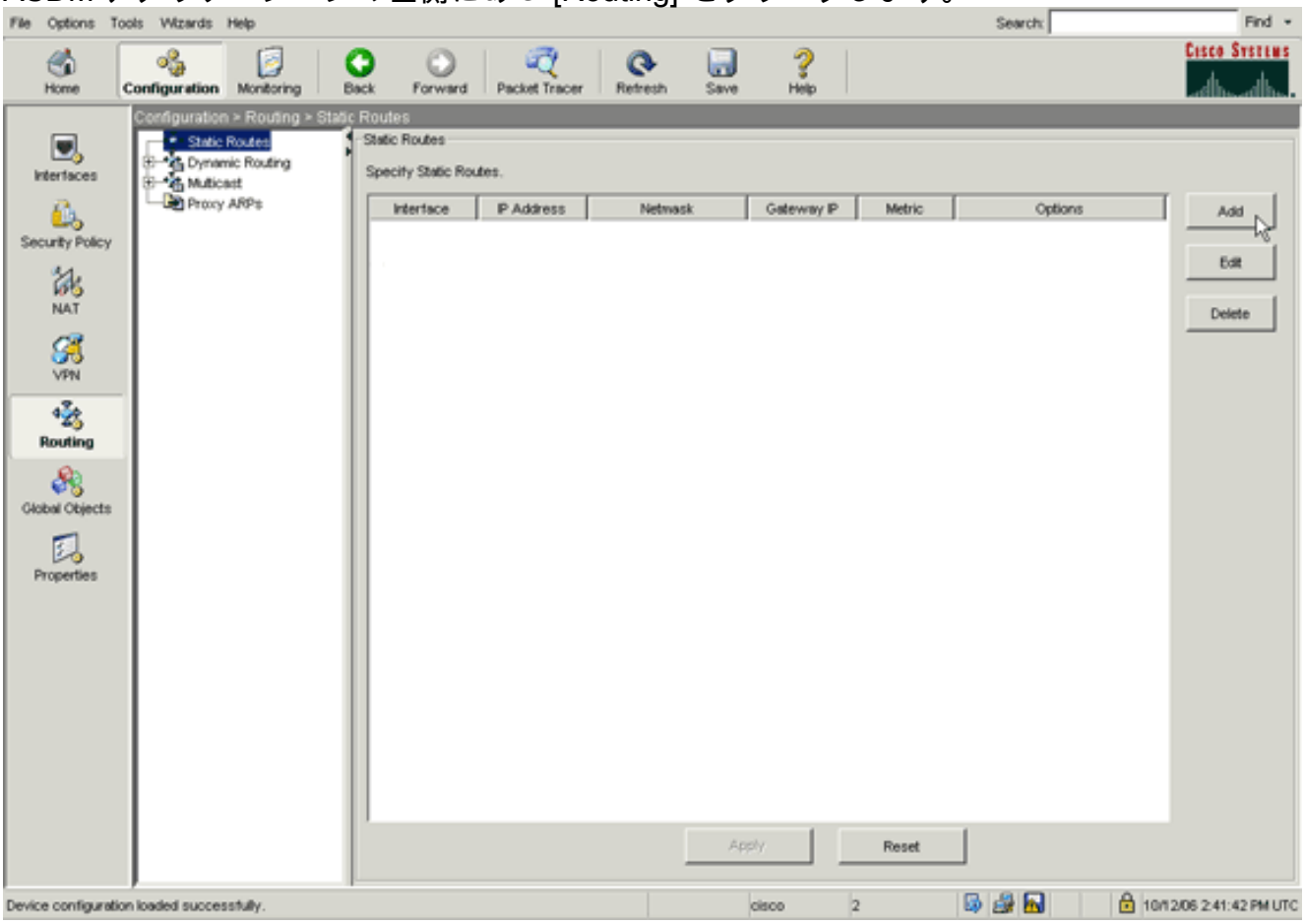
2. インターフェイスのリストから [Ethernet0] を選択して [Edit] をクリックします。次のダイアログボックスが表示されます。



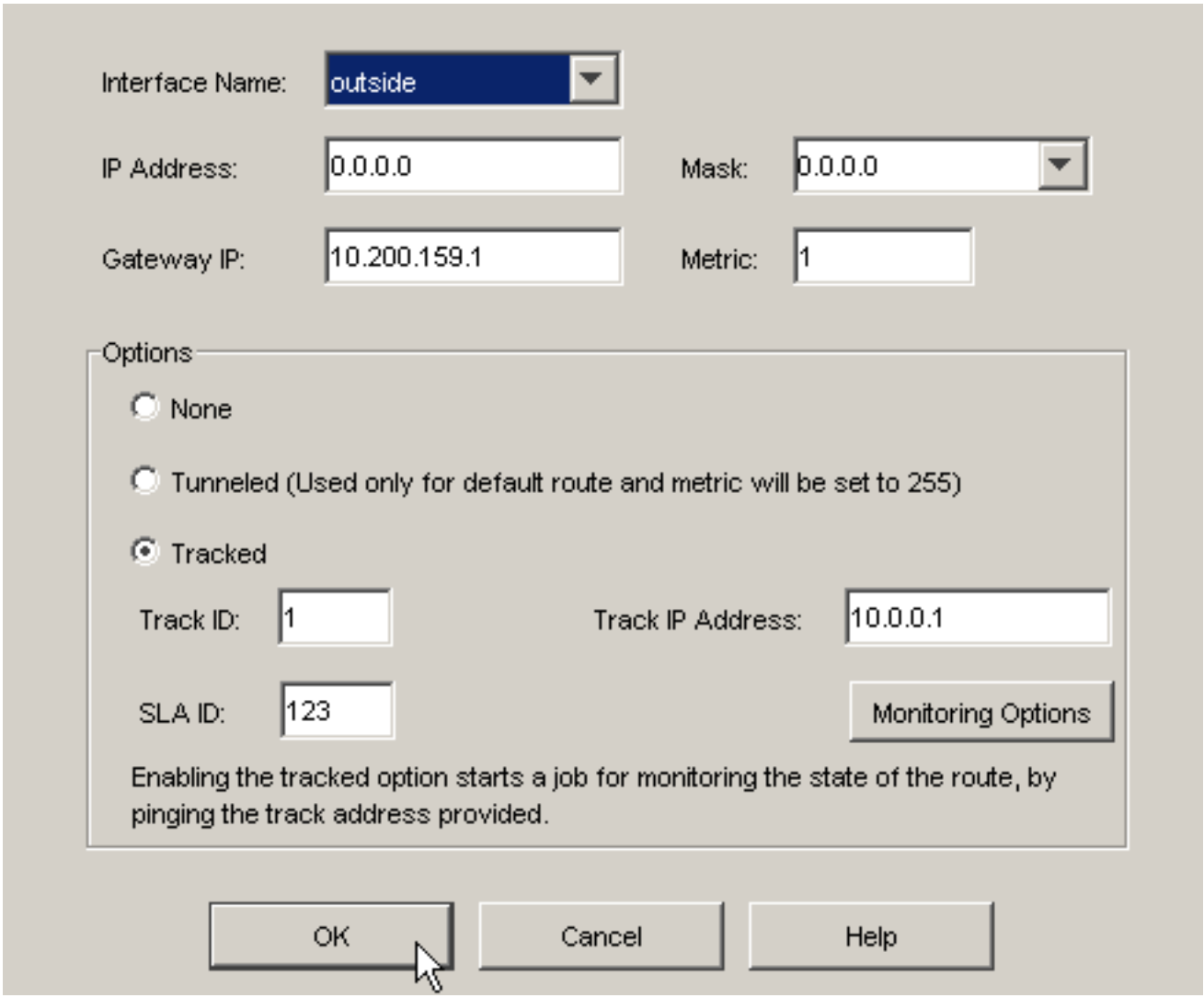
3. [Enable Interface] チェックボックスをオンにして、[Interface Name]、[Security Level]、[IP Address]、[Subnet Mask] の各フィールドに値を入力します。
4. [OK] をクリックしてダイアログボックスを閉じます。
5. 必要に応じて他のインターフェイスを設定し、[Apply] をクリックしてセキュリティ アプライアンスの設定を更新します。



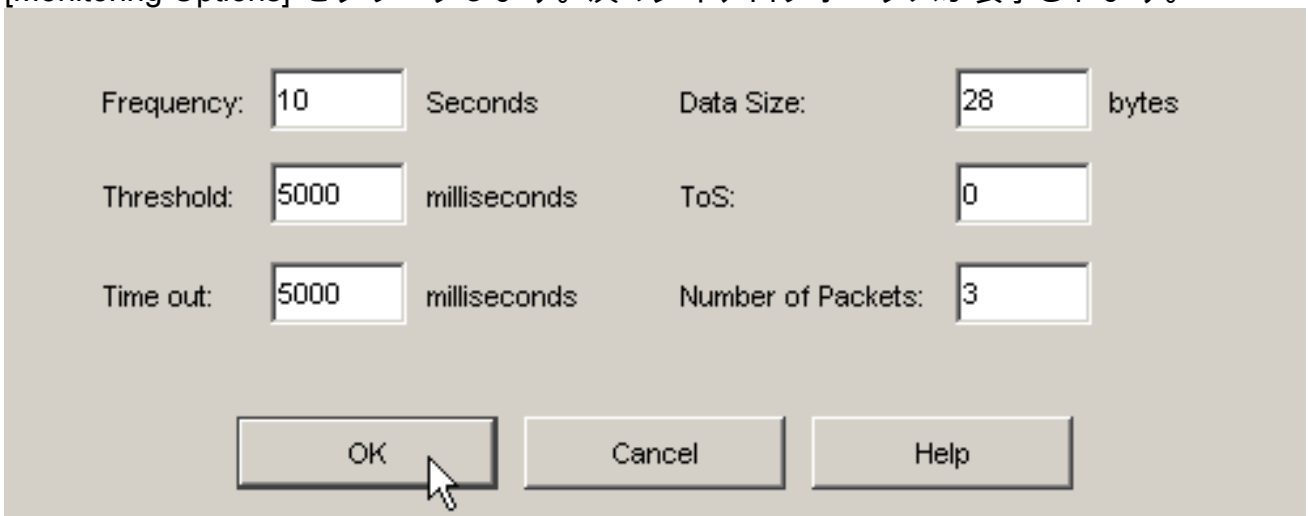
6. ASDM アプリケーションの左側にある [Routing] をクリックします。



7. [Add] をクリックして、新しいスタティック ルートを追加します。次のダイアログボックスが表示されます。



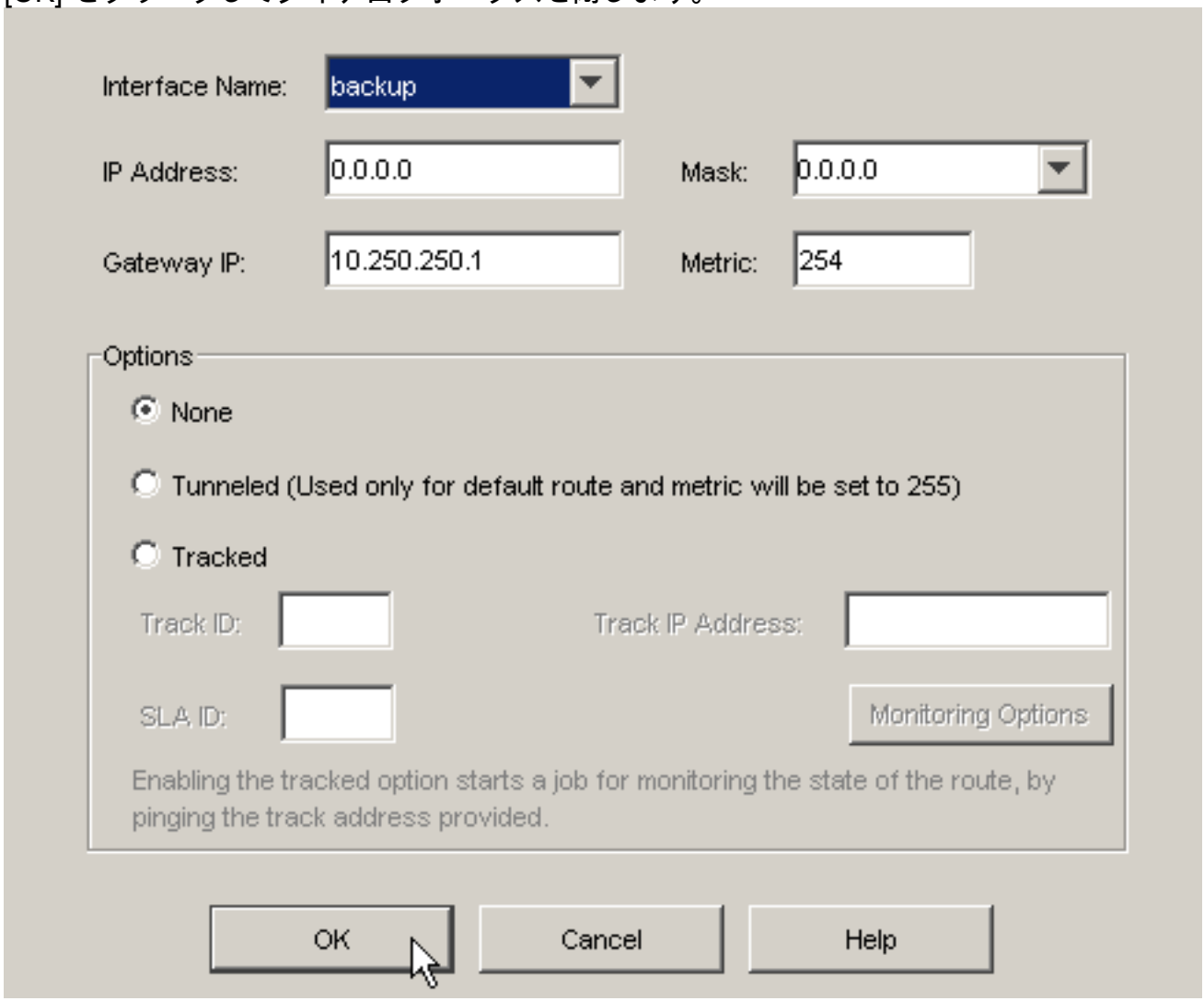
8. ルートが存在するインターフェイスを [Interface Name] ドロップダウン リストから選択し、ゲートウェイに到達するためのデフォルト ルートを設定します。 この例では、10.0.0.1 がプライマリ ISP ゲートウェイであり、ICMP エコーを使用してモニタするオブジェクトでもあります。
9. [Options] エリアで [Tracked] オプション ボタンをクリックし、[Track ID]、[SLA ID]、[Track IP Address] の各フィールドに値を入力します。
10. [Monitoring Options] をクリックします。次のダイアログボックスが表示されます。



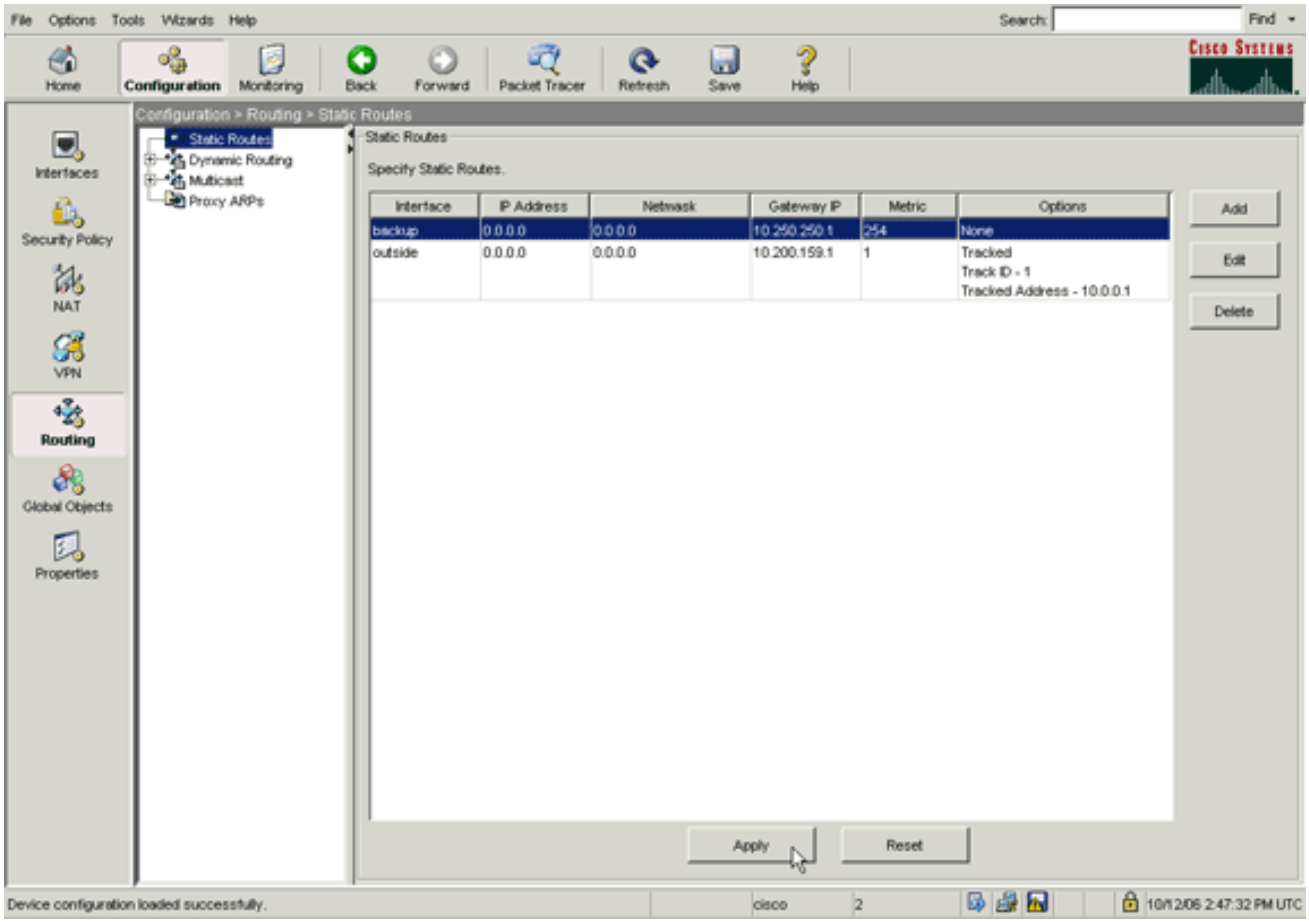
11. モニタの頻度とその他のモニタリング オプションを設定し、[OK] をクリックします。
12. セカンダリ ISP への別のスタティック ルートを追加し、インターネットに到達するためのルートを用意します。これをセカンダリ ルートにするために、このルートの設定には 254

などのより高いメトリックを使用します。 プライマリ ルート（プライマリ ISP）に障害が発生すると、このルートはルーティング テーブルから削除され、 代わりにこのセカンダリ ルート（セカンダリ ISP）が PIX のルーティング テーブルにインストールされます。

13. [OK] をクリックしてダイアログボックスを閉じます。



インターフェイス リストに設定が表示されます。



14. ルーティング設定を選択して [Apply] をクリックして、セキュリティ アプライアンスの設定を更新します。

確認

ここでは、設定が正常に動作していることを確認します。

設定が完了しているかどうかの確認

次の show コマンドを使用して、設定が完了しているかどうかを確認します。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

- **show running-config sla monitor**：設定に含まれる SLA コマンドを表示します。

```
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**：動作に関する現在の設定を表示します。

```
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 operational-state**：SLA 動作の運用統計情報を表示します。プライマリ ISP で障害が発生する前の動作ステータスは次のとおりです。

```
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
```

プライマリ ISP で障害が発生し、（ICMP エコーがタイムアウト）した後の動作ステータスは次のとおりです。

```
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
```

バックアップ ルートがインストールされているかどうかの確認（CLI を使用する方法）

show route コマンドを使用して、いつバックアップ ルートがインストールされるか確認します。

- プライマリ ISP で障害が発生する前のルーティング テーブルは次のとおりです。

```
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
```

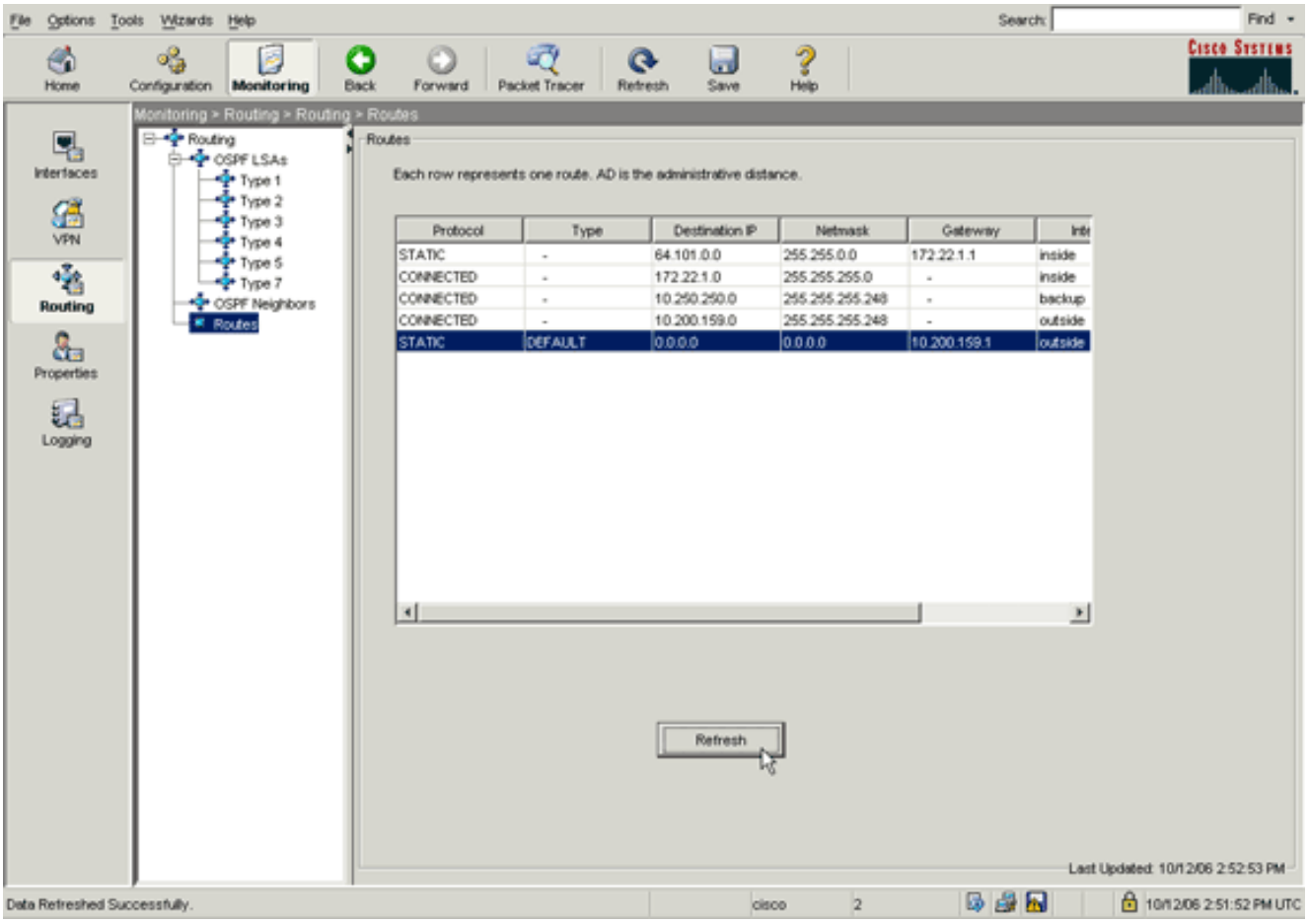
- プライマリ ISP で障害が発生した後スタティック ルートは削除され、バックアップ ルートがインストールされます。そのときのルーティング テーブルは次のとおりです。

```
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
```

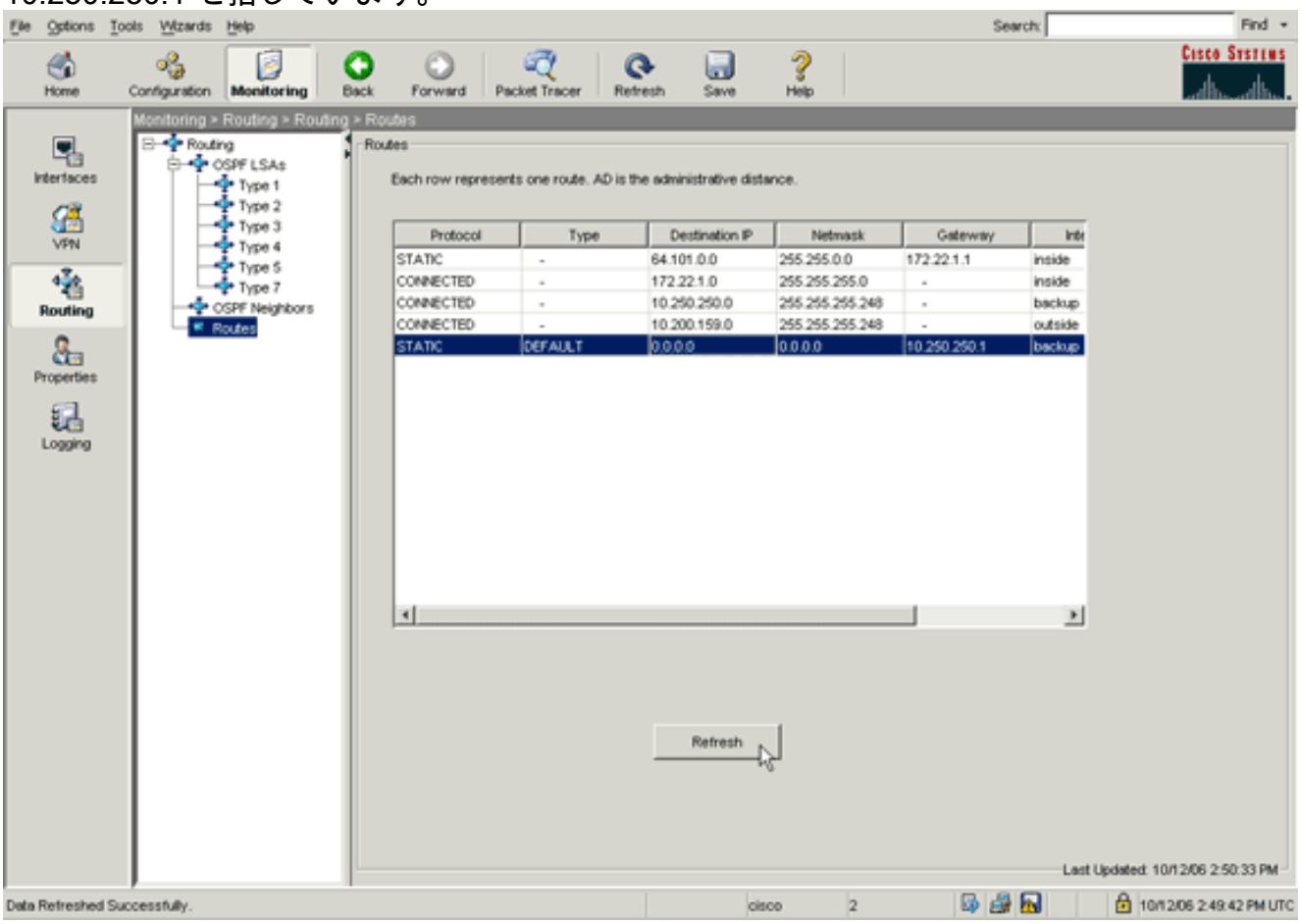
バックアップ ルートがインストールされているかどうかの確認 (ASDM を使用する方法)

バックアップ ルートがインストールされているかどうかを ASDM で確認するには、次の手順を実行します。

1. [Monitoring] をクリックし、次に [Routing] をクリックします。
2. Routing ツリーから [Routes] を選択します。プライマリ ISP で障害が発生する前のルーティング テーブルは次のとおりです。



デフォルト ルートは外部インターフェイスを経由して 10.0.0.2 を指しています。プライマリ ISP で障害が発生した後このルートは削除され、バックアップ ルートがインストールされます。 デフォルト ルートは現在、バックアップ インターフェイスを経由して 10.250.250.1 を指しています。



トラブルシューティング

debug コマンド

- **debug sla monitor trace**：エコー動作の進捗状況を表示します。トラッキング対象のオブジェクト（プライマリ ISP ゲートウェイ）は起動しているため、ICMP エコーは成功します。

```
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
```

トラッキング対象のオブジェクト（プライマリ ISP ゲートウェイ）はダウンしているため、ICMP エコーは失敗します。

```
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
```

- **debug sla monitor error**：SLA モニタ プロセスで発生したエラーを表示します。トラッキング対象のオブジェクト（プライマリ ISP ゲートウェイ）は起動しているため、ICMP は成功します。

```
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
```

トラッキング対象のオブジェクト（プライマリ ISP ゲートウェイ）はダウンしているため、トラッキング対象のルートは削除されます。

```
%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
               10.200.159.2/6405 laddr 10.200.159.2/6405
%PIX-6-302020: Built ICMP connection for faddr 10.0.0.1/0 gaddr
               10.200.159.2/6406 laddr 10.200.159.2/6406
%PIX-6-302020: Built ICMP connection for faddr 10.0.0.1/0 gaddr
               10.200.159.2/6407 laddr 10.200.159.2/6407
%PIX-6-302021: Teardown ICMP connection for faddr 10.0.0.1/0 gaddr
               10.200.159.2/6405 laddr 10.200.159.2/6405
%PIX-6-302021: Teardown ICMP connection for faddr 10.0.0.1/0 gaddr
               10.200.159.2/6406 laddr 10.200.159.2/6406
%PIX-6-302021: Teardown ICMP connection for faddr 10.0.0.1/0 gaddr
               10.200.159.2/6407 laddr 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
!--- 10.0.0.1 is unreachable, so the route to the Primary ISP is removed.
```

トラッキング対象ルートが不必要に削除される

トラッキング対象のルートが不必要に削除される場合は、モニタリング ターゲットが常に エコー要求を受信できる状態であることを確認します。 また、モニタリング ターゲットの状態（ターゲットが到達可能であるかどうか）がプライマリ ISP 接続の状態と密接に結び付いていることを確認します。

ISP ゲートウェイより遙かに遠いモニタリング ターゲットを選択すると、そのルート上にある別のリンクで障害が発生したり、別のデバイスが干渉する場合があります。 この設定が原因で、SLA モニタはプライマリ ISP への接続で障害が発生したと判断し、セキュリティ アプライアンスを不必要にセカンダリ ISP リンクにフェールオーバーさせる可能性があります。

たとえば、ブランチ オフィスのルータをモニタリング ターゲットとして選択すると、ブランチ オフィスへの ISP 接続、および途中にある別のリンクで障害が発生する可能性があります。 モニタ動作によって送信された ICMP エコーが失敗すると、プライマリ ISP リンクがまだアクティブであっても、トラッキングされていたプライマリ ルートは削除されます。

この例では、モニタリング ターゲットとして使用されているプライマリ ISP ゲートウェイは ISP によって管理され、ISP リンクの反対側に配置されています。 この設定では、モニタ動作によって送信された ICMP エコーが失敗すると、ISP リンクはほぼ確実にダウンします。

ASA での SLA モニタリング

問題：

ASA をバージョン 8.0 にアップグレードした後、SLA モニタリングが動作しません。

解決策：

この問題の原因は、おそらく **IP Reverse-Path** コマンドが**外部**インターフェイスに設定されていることにあります。 ASA のコマンドを削除して、SLA モニタリングを確認してみてください。

関連情報

- スタティック ルート トラッキングの設定
- PIX/ASA 7.2 コマンド リファレンス
- Cisco ASA 5500 シリーズ セキュリティ アプライアンス
- Cisco PIX 500 シリーズ セキュリティ アプライアンス
- テクニカル サポートとドキュメント – Cisco Systems