

ASA を冗長またはバックアップ ISP リンクに設定する

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[関連製品](#)

[背景説明](#)

[スタティックルートトラッキング機能の概要](#)

[重要な推奨事項](#)

[設定](#)

[ネットワーク図](#)

[CLI での設定](#)

[ASDM の設定](#)

[確認](#)

[設定完了の確認](#)

[バックアップルートがインストールされていることの確認 \(CLI メソッド\)](#)

[バックアップルートがインストールされていることの確認 \(ASDM メソッド\)](#)

[トラブルシューティング](#)

[デバッグコマンド](#)

[トラッキング対象のルートが不必要に削除される](#)

[関連情報](#)

はじめに

このドキュメントでは、冗長またはバックアップのインターネット接続を使用するように Cisco ASA 5500 シリーズスタティックルートトラッキング機能を設定する方法について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

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いています。


- ソフトウェア バージョン 9.x 以降を実行する Cisco ASA 5555-X シリーズ

- Cisco ASDM バージョン 7.x 以降

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

関連製品

この設定は、Cisco ASA 5500 シリーズ バージョン 9.1(5) でも使用できます。

 注:ASA 5505シリーズで4番目のインターフェイスを設定するには、backup interfaceコマンドが必要です。詳細は、『Cisco セキュリティ アプライアンス コマンド リファレンス、バージョン 7.2』の「[backup interface](#)」セクションを参照してください。

背景説明

ここでは、このドキュメントで説明されているスタティック ルート トラッキング機能の概要のほか、いくつかの重要な推奨事項について説明します。

スタティック ルート トラッキング機能の概要

スタティック ルートの問題の 1 つは、ルートがアップ状態なのかダウン状態なのかを判定する固有のメカニズムがないことです。

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、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 ルートの可用性を追跡します。

この機能は、障害発生時にルーティング テーブルからスタティック ルートを削除し、バックアップ ルートに置き換えます。

スタティック ルート トラッキングは、プライマリ専用回線が使用不能になると、ASA がセカンダリ ISP への安価な接続を使用できるようにします。

ASA は、指定された監視ターゲットにスタティック ルートを関連付けることでこの冗長性を実現します。

サービス レベル契約 (SLA) 操作は、定期的な ICMP エコー要求のターゲットを監視します。

エコー応答が返されない場合、そのオブジェクトはダウンしているものと見なされ、そのオブジ

エクトに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 ルートが使用中の場合、SLA モニタ操作は監視ターゲットへのアクセス試行を続けます。

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。

このドキュメントで使用する例では、ASA は 2 つのインターネット接続を維持します。

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 番目の接続は、セカンダリ ISP が提供する DSL モデム経由でアクセスする低速デジタル加入者線 (DSL) です。

 注：このドキュメントで説明する設定は、ASAでサポートされていないため、ロードバランシングまたはロードシェアリングには使用できません。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。

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、ASA は DSL 接続にトラフィックを転送させるようにルーティング テーブルを変更します。

スタティック ルート トラッキングは、冗長性を実現するために使用されます。

ASA には、プライマリ ISP にすべてのインターネット トラフィックを転送するスタティック ルートが設定されています。

10 秒ごとに SLA モニタ プロセスがチェックしてプライマリ ISP ゲートウェイが到達可能であることを確認します。

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。

この設定により、比較的安価な方法で ASA の背後にいるユーザがアウトバウンドのインターネットアクセスを引き続き利用できるようになります。

このドキュメントで説明されているように、この設定は常に ASA の背後にあるリソースへのインバウンドアクセスに適しているとは限りません。シームレスなインバウンド接続を実現するため、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。

重要な推奨事項


このドキュメントで説明されている設定を開始する前に、インターネット制御メッセージプロトコル (ICMP) のエコー要求に応答できる監視ターゲットを選択する必要があります。

任意のネットワークオブジェクトを選択できますが、インターネットサービスプロバイダー (ISP) の接続に密接に結びついているターゲットが推奨されます。

考えられる監視ターゲットを次に示します。


- ISP ゲートウェイアドレス
- 別の ISP-managed アドレス
- 認証、許可、アカウントティング (AAA) サーバなど、ASA がそれらと通信する別のネットワーク上のサーバ
- 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、ASA が正常に稼働しており、Cisco Adaptive Security Device Manager (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ます。

 ヒント: ASDM でデバイスを設定できるようにする方法については、『[CLIブック1: Cisco ASAシリーズの一般的な操作CLIコンフィギュレーションガイド、9.1](#)』の「ASDM用のHTTPSアクセスの設定」セクションを参照してください。

設定

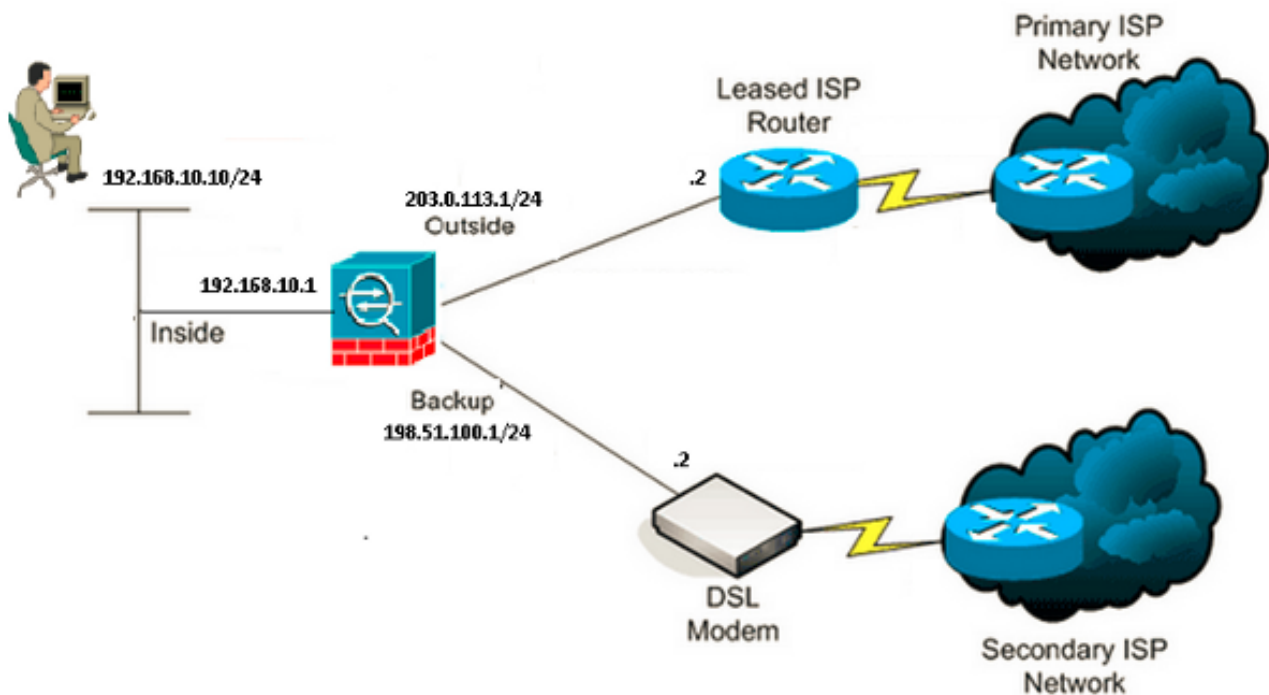
スタティックルートトラッキング機能を使用するように ASA を設定するには、この項に示す情報を参照してください。

 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。

 注: この設定で使用されている 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](#) [☐] [されます。](#) [☐]

ネットワーク図

このセクションで提供される例では、次のネットワーク設定を使用します。



CLI での設定

CLI 経由で ASA を設定するには、この情報を使用します。

```
<#root>
```

```
ASA#
```

```
show running-config
```

```
ASA Version 9.1(5)
!
hostname ASA
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 192.168.10.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif outside
 security-level 0
 ip address 203.0.113.1 255.255.255.0
!
interface GigabitEthernet0/2
 nameif backup
 security-level 0
```

```
ip address 198.51.100.1 255.255.255.0
```

```
!--- The interface attached to the Secondary ISP.
```

```
!--- "backup" was chosen here, but any name can be assigned.
```

```
!  
interface GigabitEthernet0/3  
shutdown  
no nameif  
no security-level  
no ip address  
!  
interface GigabitEthernet0/4  
no nameif  
no security-level  
no ip address  
!  
interface GigabitEthernet0/5  
no nameif  
no security-level  
no ip address  
!  
interface Management0/0  
management-only  
no nameif  
no security-level  
no ip address  
!  
boot system disk0:/asa915-smp-k8.bin  
ftp mode passive  
clock timezone IND 5 30  
object network Inside_Network  
subnet 192.168.10.0 255.255.255.0  
object network inside_network  
subnet 192.168.10.0 255.255.255.0  
pager lines 24  
logging enable  
mtu inside 1500  
mtu outside 1500  
mtu backup 1500  
icmp unreachable rate-limit 1 burst-size 1  
no asdm history enable  
arp timeout 14400  
no arp permit-nonconnected  
!  
object network Inside_Network  
nat (inside,outside) dynamic interface  
object network inside_network  
nat (inside,backup) dynamic interface
```

```
!--- NAT Configuration for Outside and Backup
```

```
route outside 0.0.0.0 0.0.0.0 203.0.113.2 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 0.0.0.0 198.51.100.2 254
```

!--- 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 pat-xlate 0:00:30
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 sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
```

```
sla monitor 123
 type echo protocol ipIcmpEcho 4.2.2.2 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.
```

```
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
!
track 1 rtr 123 reachability
```

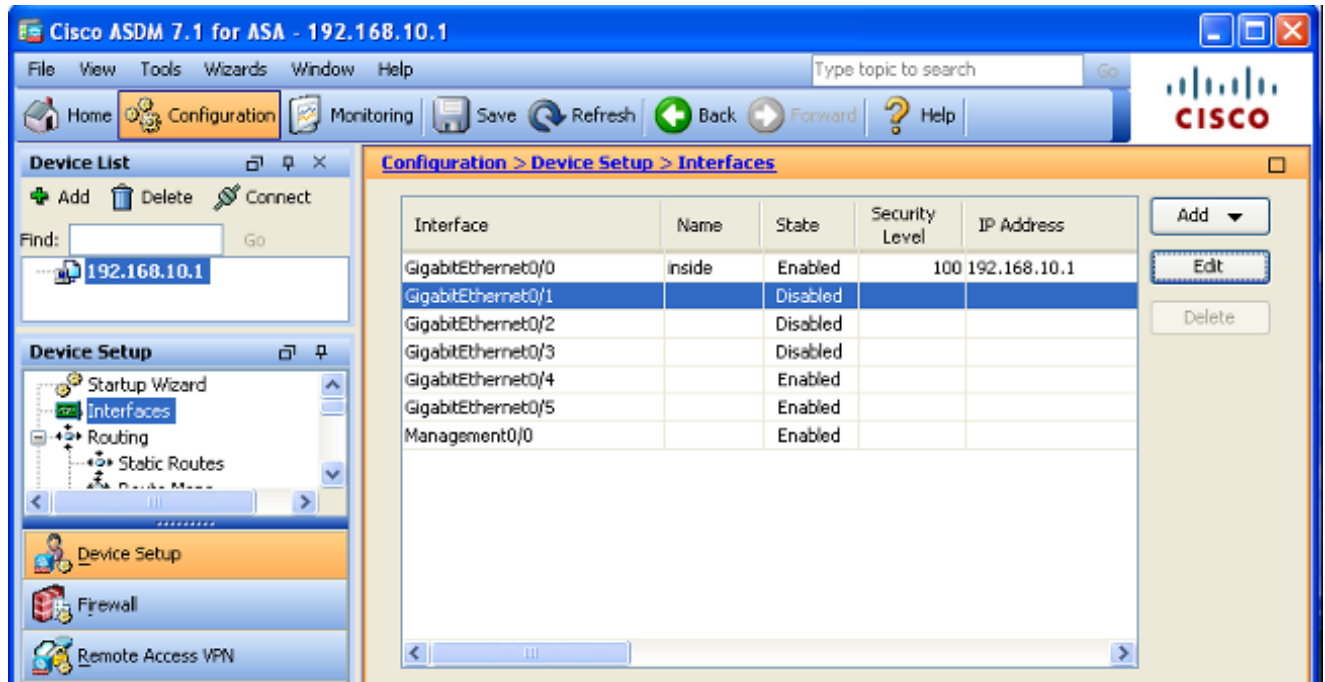
```
!--- Associate a tracked static route with the SLA monitoring process.
!--- The track ID corresponds to the track ID given to the static route to monitor:
!--- route outside 0.0.0.0 0.0.0.0 10.0.0.2 1 track 1
!--- "rtr" = Response Time Reporter entry. 123 is the ID of the SLA process
!--- defined above.
```

```
telnet timeout 5
ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
priority-queue inside
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  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 rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
!
service-policy global_policy global
```

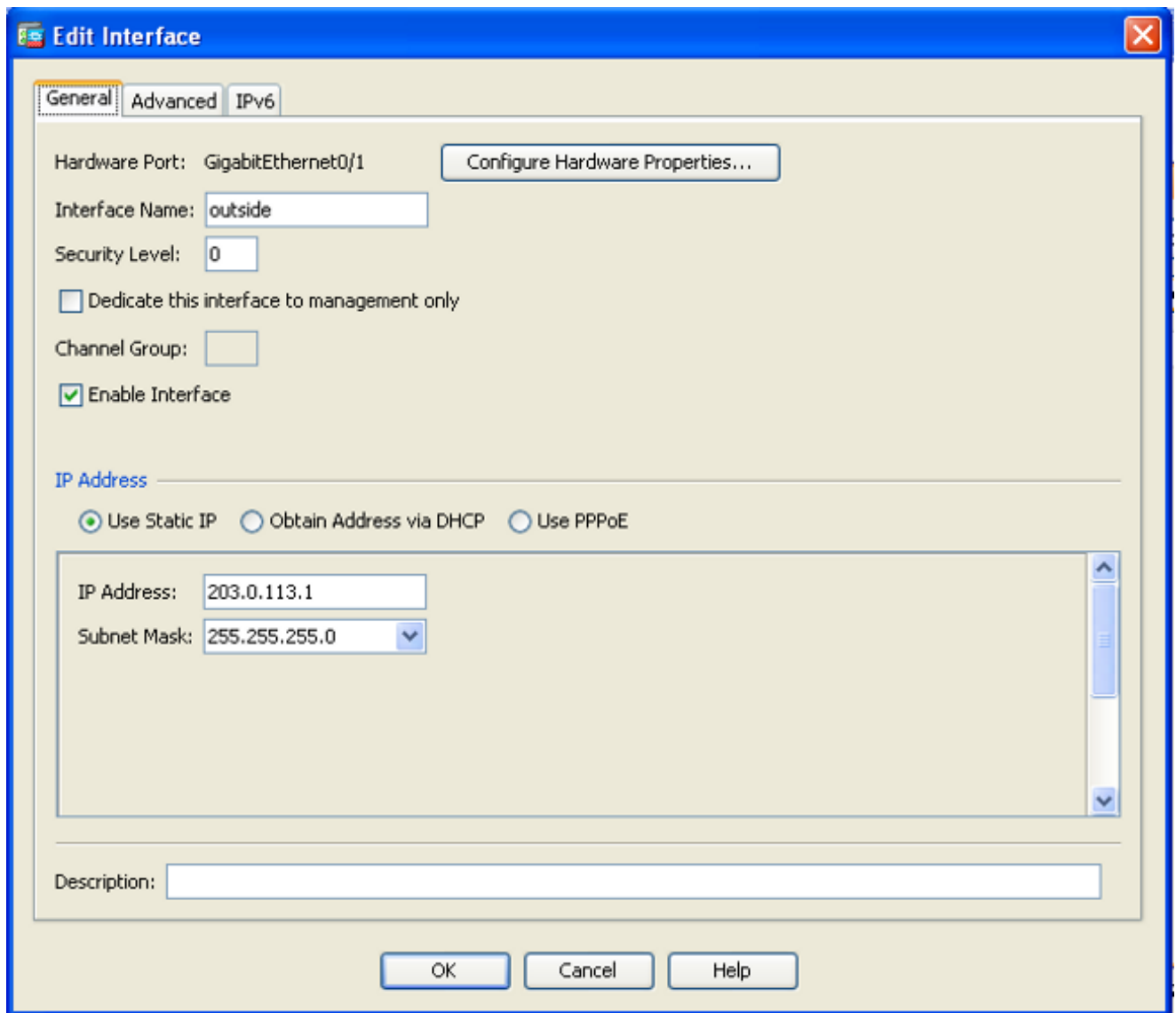

ASDM の設定

[ASDM アプリケーションを使用して冗長またはバックアップ ISP サポートを設定するには、次の手順を実行してください。](#)

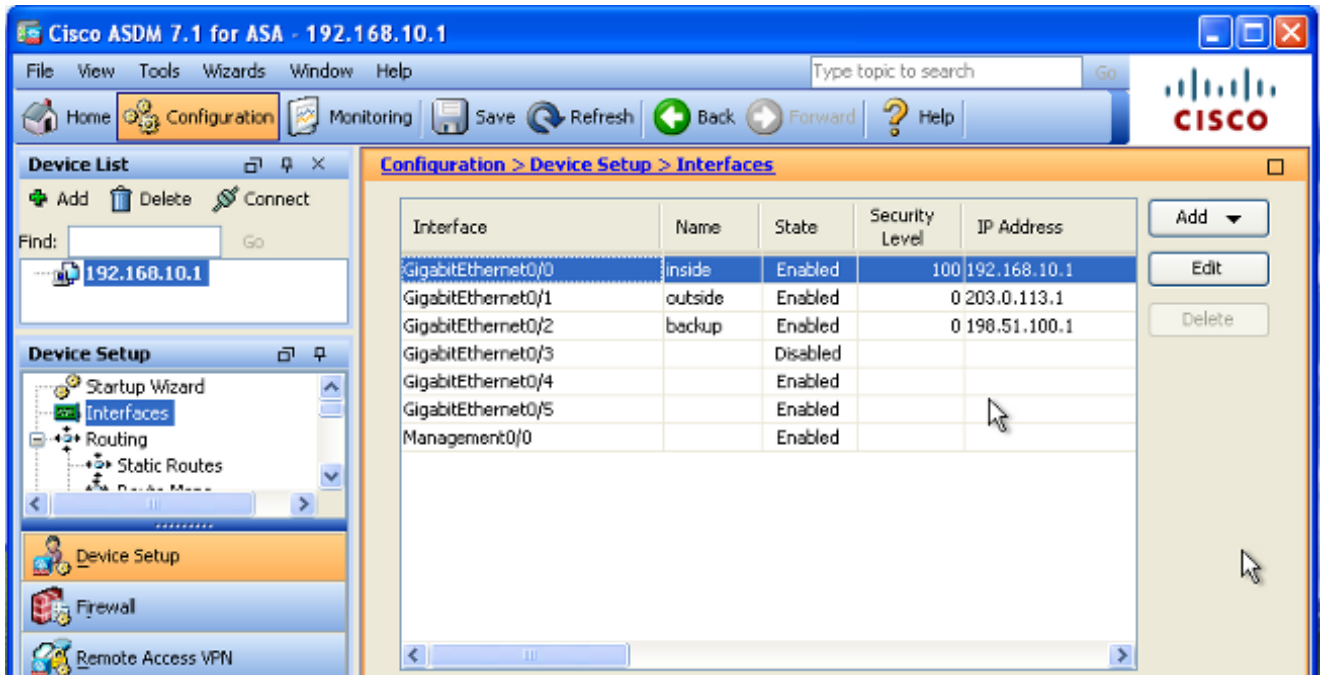
1. ASDM アプリケーション内で [Configuration] をクリックし、次に [Interfaces] をクリックします。



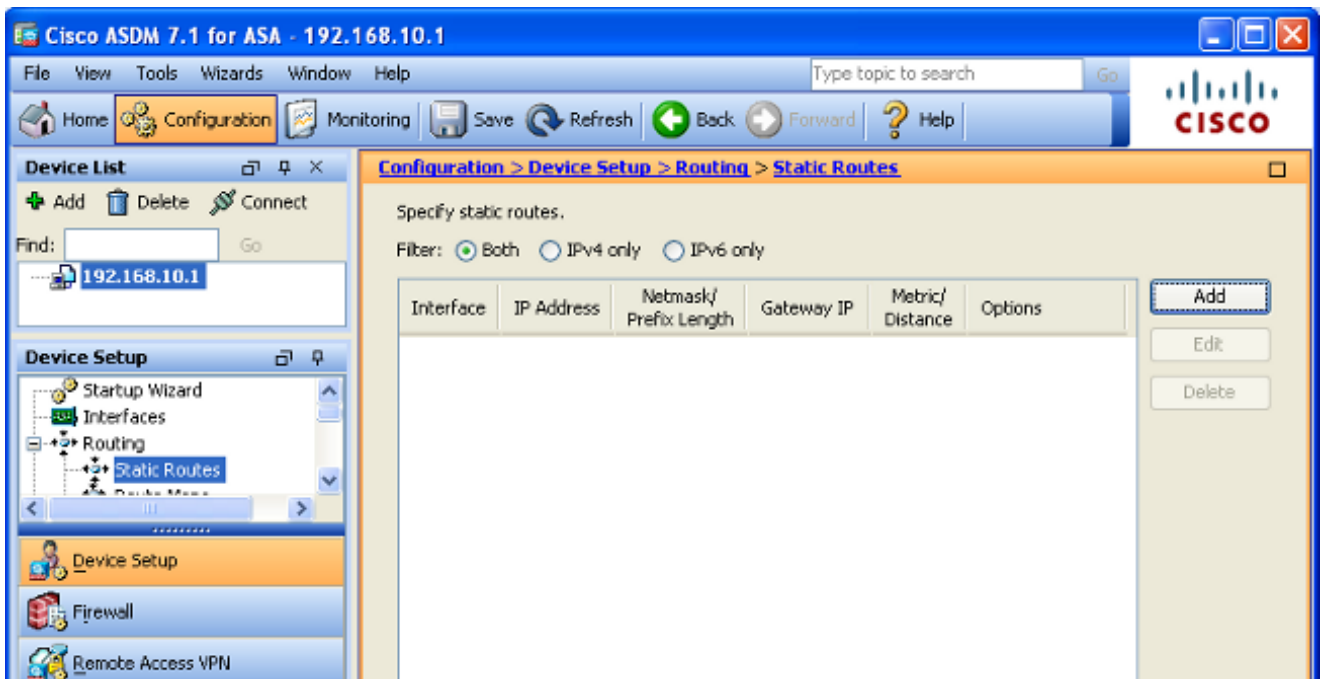
2. インターフェイス リストから [GigabitEthernet0/1] を選択し、[Edit] をクリックします。ダイアログボックスが表示されます。



3. [Enable Interface] チェックボックスをオンにして、[Interface Name]、[Security Level]、[IP Address]、および [Subnet Mask] の各フィールドに適切な値を入力します。
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 ASA 設定をアップデートします。



6. [Routing] を選択して、ASDM アプリケーションの左側にある [Static Routes] 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。ダイアログボックスが表示されます。

Edit Static Route

IP Address Type: IPv4 IPv6

Interface:

Network:

Gateway IP: Metric:

Options

None

Tunneled (Default tunnel gateway for VPN traffic)

Tracked

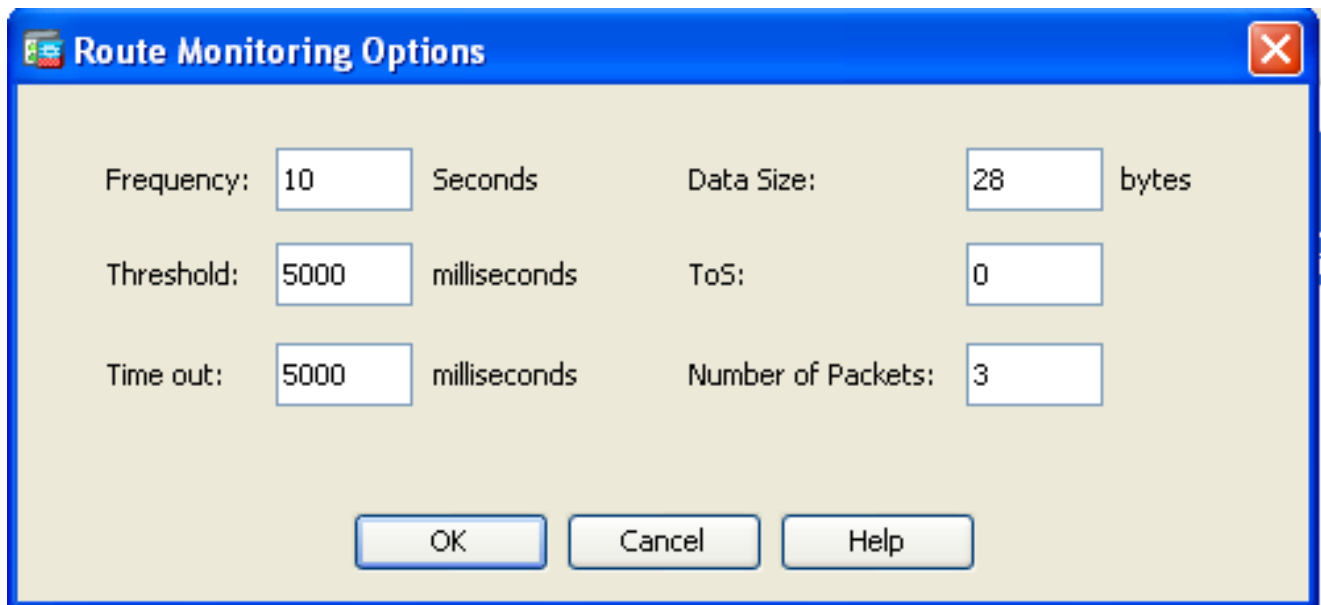
Track ID: Track IP Address:

SLA ID: Target Interface:

Monitoring Options

Enabling the tracked option starts a job for monitoring the state of the route, by pinging the track address provided.

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、203.0.113.2 がプライマリ ISP ゲートウェイで、4.2.2.2 が ICMP エコーを使用して監視するオブジェクトです。
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]、および [Track IP Address] の各フィールドに適切な値を入力します。
10. [Monitoring Options] をクリックします。ダイアログボックスが表示されます。



11. 頻度などの監視オプションに適切な値を入力し、[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 Private Internet Exchange (PIX) 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。

Edit Static Route

IP Address Type: IPv4 IPv6

Interface: backup

Network: any4

Gateway IP: 198.51.100.2 Metric: 254

Options

None

Tunneled (Default tunnel gateway for VPN traffic)

Tracked

Track ID: Track IP Address:

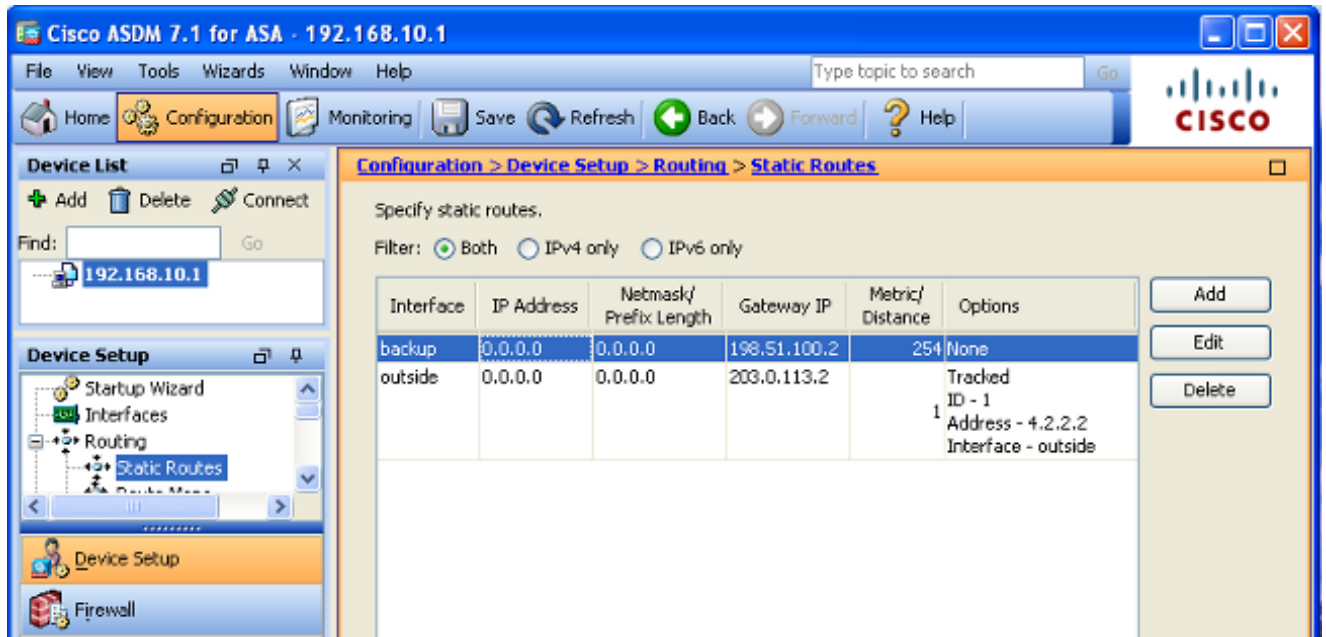
SLA ID: Target Interface: backup

Monitoring Options

Enabling the tracked option starts a job for monitoring the state of the route, by pinging the track address provided.

OK Cancel Help

設定がインターフェイス リストに表示されます。




14. ルーティング設定を選択し、[Apply] をクリックして ASA 設定をアップデートします。

確認

ここでは、設定が正常に機能しているかどうかを確認します。

設定完了の確認

 注：特定の [show](#) コマンドが、[Output Interpreter Tool](#)(登録ユーザ専用)でサポートされています。show コマンドの出力の分析を表示するには、Output Interpreter Tool を使用します。

設定が完了したことを確認するには、次の show コマンドを使用します。

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

```
<#root>
```

```
ASA#
```

```
show running-config sla monitor
```

```
sla monitor 123
```

```
type echo protocol ipIcmpEcho 4.2.2.2 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。

<#root>

ASA#

```
show sla monitor configuration 123
```

```
IP SLA Monitor, Infrastructure Engine-II.  
Entry number: 123  
Owner:  
Tag:  
Type of operation to perform: echo  
Target address: 4.2.2.2  
Interface: outside  
Number of packets: 3  
Request size (ARR data portion): 28  
Operation timeout (milliseconds): 5000  
Type Of Service parameters: 0x0  
Verify data&colon; 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。

<#root>

ASA#

```
show sla monitor operational-state 123
```

```
Entry number: 123  
Modification time: 13:30:40.672 IND Sun Jan 4 2015  
Number of Octets Used by this Entry: 2056  
Number of operations attempted: 46  
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: 13:38:10.672 IND Sun Jan 4 2015
```


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 に障害が発生 (および ICMP エコーがタイムアウト) した後の動作状態は次のとおりです。

<#root>

ASA#

show sla monitor operational-state

```
Entry number: 123
Modification time: 13:30:40.671 IND Sun Jan 4 2015
Number of Octets Used by this Entry: 2056
Number of operations attempted: 57
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: 13:40:00.672 IND Sun Jan 4 2015

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ことの確認 (CLI メソッド)

バックアップ ルートがインストールされたことを確認するには、次の show route コマンドを入力します。

プライマリ ISP に障害が発生する前は、次のようなルーティング テーブルが表示されます。

```
<#root>
```

```
ASA#
```

```
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 203.0.113.2 to network 0.0.0.0
```

```
C 203.0.113.0 255.255.255.0 is directly connected, outside  
C 192.168.10.0 255.255.255.0 is directly connected, inside  
C 198.51.100.0 255.255.255.0 is directly connected, backup  
s* 0.0.0.0 0.0.0.0 [1/0] via 203.0.113.2, outside
```

プライマリ ISP に障害が発生し、スタティックルートが削除され、バックアップルートがインストールされた後は、次のようなルーティングテーブルが表示されます。

```
<#root>
```

```
ASA#
```

```
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 198.51.100.2 to network 0.0.0.0
```

```
C 203.0.113.0 255.255.255.0 is directly connected, outside  
C 192.168.10.0 255.255.255.0 is directly connected, inside  
C 198.51.100.0 255.255.255.0 is directly connected, backup  
s* 0.0.0.0 0.0.0.0 [254/0] via 198.51.100.2, backup
```

バックアップルートがインストールされていることの確認 (ASDM メソッド)

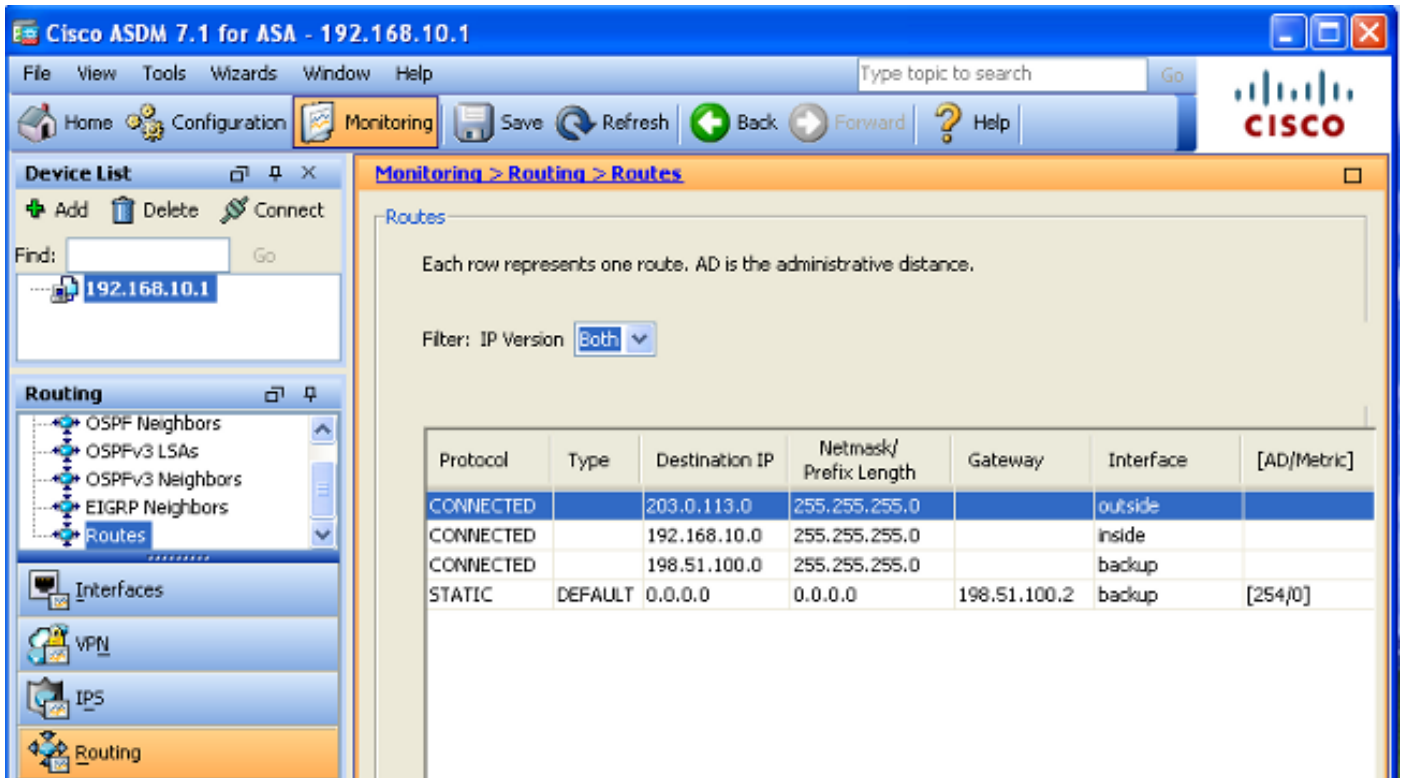
バックアップルートが ASDM 経由でインストールされていることを確認するには、[Monitoring] > [Routing] に移動し、[Routing] ツリーから [Routes] を選択します。

プライマリ ISP に障害が発生する前は、次の画像のようなルーティングテーブルが表示されます。デフォルトルートが外部インターフェイスを介して 203.0.113.2 を指定していることに注意してください。

The screenshot shows the Cisco ASDM 7.1 for ASA interface. The left sidebar contains a 'Device List' with '192.168.10.1' selected and a 'Routing' tree with 'Routes' selected. The main content area is titled 'Monitoring > Routing > Routes' and displays a table of routes. The table has columns for Protocol, Type, Destination IP, Netmask/Prefix Length, Gateway, Interface, and [AD/Metric].

Protocol	Type	Destination IP	Netmask/Prefix Length	Gateway	Interface	[AD/Metric]
CONNECTED		203.0.113.0	255.255.255.0		outside	
CONNECTED		192.168.10.0	255.255.255.0		inside	
CONNECTED		198.51.100.0	255.255.255.0		backup	
STATIC	DEFAULT	0.0.0.0	0.0.0.0	203.0.113.2	outside	[1/0]

プライマリ ISP に障害が発生し、ルートが削除され、バックアップルートがインストールされた後の状態です。デフォルトルートがバックアップインターフェイスを介して 198.51.100.2 を指定するようになっています。



トラブルシュート

このセクションでは、便利な debug コマンドを紹介し、監視対象のルートが不必要に削除される問題をトラブルシューティングする方法を説明します。

デバッグ コマンド

次のデバッグ コマンドを使用して、設定に関する問題のトラブルシューティングを行うことができます。

- debug sla monitor trace : エコー処理の進捗を表示します。
 - トラッキング対象オブジェクト (プライマリ ISP ゲートウェイ) がアップ状態で ICMP エコーに成功すると、次のような出力が表示されます。

```
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=0 OK
IP SLA Monitor(123) echo operation: RTT=0 OK
IP SLA Monitor(123) echo operation: RTT=1 OK
IP SLA Monitor(123) Scheduler: Updating result
```

- トラッキング対象オブジェクト (プライマリ ISP ゲートウェイ) がダウン状態で ICMP エコーに失敗すると、次のような出力が表示されます。

```
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 : SLA モニタ プロセスで発生したエラーを表示します。

- トラッキング対象オブジェクト (プライマリ ISP ゲートウェイ) がアップ状態で ICMP に成功すると、次のような出力が表示されます。

```
%ASA-7-609001: Built local-host identity:203.0.113.1
%ASA-7-609001: Built local-host outside:4.2.2.2
%ASA-6-302020: Built outbound ICMP connection for faddr 4.2.2.2/0
gaddr 203.0.113.1/39878 laddr 203.0.113.1/39878
%ASA-6-302021: Teardown ICMP connection for faddr 4.2.2.2/0 gaddr
203.0.113.1/39878 laddr 203.0.113.1/39878
%ASA-7-609002: Teardown local-host identity:203.0.113.1 duration 0:00:00
%ASA-7-609002: Teardown local-host outside:4.2.2.2 duration 0:00:00
%ASA-7-609001: Built local-host identity:203.0.113.1
%ASA-7-609001: Built local-host outside:4.2.2.2
%ASA-6-302020: Built outbound ICMP connection for faddr 4.2.2.2/0
gaddr 203.0.113.1/39879 laddr 203.0.113.1/39879
%ASA-6-302021: Teardown ICMP connection for faddr 4.2.2.2/0 gaddr
203.0.113.1/39879 laddr 203.0.113.1/39879
%ASA-7-609002: Teardown local-host identity:203.0.113.1 duration 0:00:00
%ASA-7-609002: Teardown local-host outside:4.2.2.2 duration 0:00:00
```

- トラッキング対象オブジェクト (プライマリ ISP ゲートウェイ) がダウン状態でトラッキング対象ルートが削除されると、次のような出力が表示されます。

<#root>

```
%ASA-7-609001: Built local-host identity:203.0.113.1
%ASA-7-609001: Built local-host outside:4.2.2.2
%ASA-6-302020: Built outbound ICMP connection for faddr 4.2.2.2/0
gaddr 203.0.113.1/59003 laddr 203.0.113.1/59003
%ASA-6-302020: Built outbound ICMP connection for faddr 4.2.2.2/0
gaddr 203.0.113.1/59004 laddr 203.0.113.1/59004
%ASA-6-302020: Built outbound ICMP connection for faddr 4.2.2.2/0
gaddr 203.0.113.1/59005 laddr 203.0.113.1/59005
%ASA-6-302021: Teardown ICMP connection for faddr 4.2.2.2/0 gaddr
203.0.113.1/59003 laddr 203.0.113.1/59003
%ASA-6-302021: Teardown ICMP connection for faddr 4.2.2.2/0 gaddr
203.0.113.1/59004 laddr 203.0.113.1/59004
%ASA-6-302021: Teardown ICMP connection for faddr 4.2.2.2/0 gaddr
203.0.113.1/59005 laddr 203.0.113.1/59005
%ASA-7-609002: Teardown local-host identity:203.0.113.1 duration 0:00:02
%ASA-7-609002: Teardown local-host outside:4.2.2.2 duration 0:00:02
%ASA-6-622001: Removing tracked route 0.0.0.0 0.0.0.0 203.0.113.2,
distance 1, table Default-IP-Routing-Table, on interface outside
```

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

トラッキング対象の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ゲートウェイよりも遠いモニタリングターゲットを選択すると、そのルート上の別のリンクで障害が発生したり、別のデバイスで干渉が発生したりする可能性があります。

したがって、この設定により、SLAモニタは、プライマリISPへの接続に障害が発生したと判断し、ASAがセカンダリISPリンクに不必要にフェールオーバーす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。

監視操作によって送信された ICMP エコーに障害が発生した場合、プライマリ ISP リンクがまだアクティブであっても、トラッキング対象のプライマリ 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、監視操作によって送信された ICMP エコーに障害が発生した場合、ISP リンクがほぼ確実にダウンするようになります。

関連情報

- [Cisco ASA 5500-X シリーズ次世代ファイアウォール](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。