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 前提条件 要件 使用するコンポーネント 関連製品 表記法 背景説明 設定 ネット<u>ワーク図</u> 設定 CLI 設定 ASDM の設定 確認 設定が完了しているかどうかの確認 <u>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)</u> 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) トラブルシューティング debug コマンド トラッキング対象ルートが不必要に削除される ASA での SLA モニタリング 関連情報

<u>はじめに</u>

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

<u>要件</u>

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、『<u>ASDM 用の HTTPS ア</u> <u>クセスの許可</u>』を参照してください。

<u>使用するコンポーネント</u>

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。 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「<u>backup interface</u>」を参照してください。

<u>表記法</u>

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

<u>背景説明</u>

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。

<u>設定</u>

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 <u>RFC 1918</u> 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 。



```
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。
```



<u>設定</u>

このドキュメントでは、次の設定を使用します。

- <u>コマンドライン インターフェイス (CLI)</u>
- 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、<u>Command Lookup Tool</u>(<u>登</u> <u>録</u>ユーザ専用)を使用してください。

<u>CLI 設定</u>

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
!
1
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
```

<u>ASDM の設定</u>

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。

Image: Security Policy I	
Configuration > Interfaces Interfaces Interface Name Enabled Security Level P Address Subnet Mask Management Only MTU Active MAC Address Stan MAC A Security Policy Ethernet1 backup Yes 0 10/200/159/2 255/255/255/248 No 1,500 Imagement MAC	alla
Interfaces Interface Name Enabled Security Level P Address Subnet Mask Management Only MTU Active MAC Address Stan MAC A Image: Security Policy Ethernet1 backup Yes 0 10/200/159/2 255/255/256/248 No 1,500 - Image: Security Policy Ethernet1 backup Yes 0 10/250/250/2 255/255/256/248 No 1,500 - Image: Security Policy Ethernet3 Inside Yes 100 172/221.163 255/255/256.0 No 1,500 - Image: Security Policy Ethernet3 No 0 172/221.163 255/255/255.0 No 1,500 - - Image: Security Policy Ethernet4 No - - No - - - Image: NAT No No - - No - - - -	
Ethernet0 outside Yes 0 10 200 159 2 255 255 255 248 No 1,500 Security Policy Ethernet1 backup Yes 0 10 250 250 2 255 255 255 248 No 1,500 - Librard Inside Yes 0 10 250 250 2 255 255 255 0 No 1,500 - Librard Inside Yes 100 172 221 163 255 255 255 0 No 1,500 - Librard No No No No - - - NAT Ethernet5 No No No - - -	Add
Ethernet1 backup Yes 0 10 250 250 2 255 255 254 8 No 1,500	Edit N
Security Policy Uthermet2 inside Yes 100 172 221.163 255.255.255.0 No 1,500 Bthermet3 Nio N	-13
EthernetS No No Bhernet4 No No Bhernet5 No No	elete
NAT EthernetS No No	
NAT CONTRACT THE THE THE	
Global Objects Properties	
Apply Reset	
cisco 2 😡 🍰 🔂 10/12/06/21/0	52 PM UTC

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。

Enable Interface	Dedicate this interface to	management only	
nterface Name: ou	tside	Security Level:	0
P Address	C Obtain Address via DHCP	C Use	PPPoE
IP Address:	10.200.159.2		
Subnet Mask:	255.255.255.248		
escription: I			

- 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。

File Options To	ols Wizards Help							s	earch:		Find +
Home (Configuration Monitoring	Back I	Forward	Racket Tra	cer Refresh	Save Help				Cu	co Systems Anadra
	Configuration > Interfaces										
E,	Interface	Name	Enabled	Security Level	IP Address	Subnet Mask	Management Only	MTU	Active MAC Address	Stan MAC A	Add
	Ethernet0	outside	Yes	0	10.200.159.2	255.255.255.248	No	1,500			For
<u>6</u> ,	Ethernet1	backup	Yes	0	10.250.250.2	255.255.255.248	No	1,500			
Security Policy	Ethernet2	inside	Yes	100	172.22.1.163	255.255.255.0	No	1,500			Delete
	Ethernet3		No				No				
Cake 1	Ethernet4		No				No				
NAT	Ethernet5		No				No				
Global Objects	1										
	Enable traffic between tw	o or more inter	faces which	are config	ared with same sec	curity levels					
	Enable traffic between to	o or more bost	is connected	to the serve	e interface						
		o or more ride	a corrected	to the odds	Apply	Reset					
Device configuratio	n loaded successfully.					cisco	2	5 d		10/12/06 2	20:52 PM UTC

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。

File Options To	ols Wizards	Help							Search	Find +
Home	ogg Configuration	Monitoring	Back For	vard Packet Trace	Retresh	Save	? Help			Cisco Systems
Interfaces Security Policy NAT Security Policy NAT Security Policy NAT Security NAT Security Properties	Coordiguratio	n > Routing > St Routes mic Routing sat y ARPs	atic Routes Static Route Specify Stat	s ic Routes. ie P Address	Netwask	K Appi	Gateway P	Reset	Options	Add Edit Delete
Device configuration	n inaded succe	antidu.				6	ison .	2		A 10/12/06 241:42 PM LTD

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。

Interface Name:	outside]	
IP Address:	0.0.0.0	Mask:	0.0.0.0
Gateway IP:	10.200.159.1	Metric:	1
Options			
C None			
C Tunneled (L	lsed only for default route	and metric wil	be set to 255)
Tracked		en al ID A dalen au	40.0.0.4
		ack IP Addres:	s: 10.0.0.1
SLA ID: 12	23		Monitoring Options
Enabling the tra pinging the trac	icked option starts a job fo x address provided.	or monitoring th	e state of the route, by
<u>.</u>			

- 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。

Frequency:	10	Seconds	Data Size:	28	bytes
Threshold:	5000	milliseconds	ToS:	0	
Time out:	5000	milliseconds	Number of Packets:	3	
	ок	Can	cel He	lp	

 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	を閉じる	ます。
--	-----	------	----	----	----	-----	-----	-----	----	------	-----

n Address.	0.0.0.0	Mask:	0.0.0.0
Gateway IP:	10.250.250.1	Metric:	254
Options			
None			
C Tunneled	(Used only for default rout	e and metric w	ill be set to 255)
C Tracked			
Track ID:		Track IP Addres	35:
SLA ID:			Monitoring Option
Enabling the t	racked option starts a job	for monitoring t	he state of the route, by

インターフェイス リストに設定が表示されます。

File Options To	is Wizards	Help							Search	Find •
Home d	oggi Configuration	Monitoring E	C O Back Forward	Packet Tracer	Refresh	Save	? Help			Cisco Systems
Interfaces Interfaces Security Policy NAT Security Policy NAT Security Policy NAT Security Policy Properties	Configuration State S	h > Routing > Site Route: mic Routing att .ARPs	C Routes -Static Routes Specify Static Ro Interface backup outside	Autors.	Netwasi	k API	Gateway IP 10 250 250 1 10 200 159 1	Metric 254 1 Reset	Options None Tracked Tracked Address - 10.0.0.1	Add EdR Delete
Device configuration	loaded succe	sstully.					cisco	2	🔯 🎒 🔂 🛛 🔂 10	0/12/06 2:47:32 PM UTC

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。

<u>確認</u>

ここでは、設定が正常に動作していることを確認します。

<u>設定が完了しているかどうかの確認</u>

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。

<u>Output Interpreter Tool</u>(OIT)(<u>登録</u>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:
              RTTMin: 0
                              RTTMax: 0
 RTTAva: 0
 NumOfRTT: 0 RTTSum: 0
                               RTTSum2: 0
```



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 10.250.250.0 255.255.248 is directly connected, backup
- C 10.200.159.0 255.255.248 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 10.250.250.0 255.255.248 is directly connected, backup
- C 10.200.159.0 255.255.248 is directly connected, outside
- S* 0.0.0.0 0.0.0.0 [254/0] via 10.250.250.1, backup

<u>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)</u>

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。

File Options Tools M	tzards <u>H</u> elp						See	wch:	Find +
Home Config	nation Monitoring	Back	Forward Pa	Cket Tracer Ref	> 📄	? Help			Cisco Status
Interfaces WPN Routing Properties Logging	Oring > Routing > R Routing - OSPF LSAs - Type 1 - Type 2 - Type 3 - Type 7 - Type 7 - CSPF Neighbor - Routes	s	Ares Each row represent Each row represent STATIC CONNECTED CONNECTED STATIC INNECTED STATIC INNECTED	ts one route. AD is t Type - - - CEPAULT	e administrative dist Destination IP 64.101.0.0 172.22.1.0 10.250.250.0 10.200.159.0 00.000	ance. 255 255 0 255 255 255 243 255 255 255 243 0 0.0 0	Cateway 172:22:1.1 - - 10:200.169:1	Intr Inside Inside Deckup Outside Outside	Jpdatlest: 10/1206 2:52:53 PM
Data Refreshed Successful	₿y.				cis	100 2	😡 🞒	20	10/12/06 2:51:52 PM UTC

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。

File Options	Tools Wizards	Help						Se	arch:	Find •
Showe	Configuration	Monitoring	O Back	Forward P	acket Tracer F	💽 🔜 Intresh Save	? Help			Cisco Statius
Routing Properties Logging		 Routing > Routing > Routing > Routing > Routing > Type 1 Type 1 Type 2 Type 3 Type 4 Type 5 Type 7 OSPF Neighbors Route 	Fine Ro	LODIS Ares Each row represe STATIC CONNECTED CONNECTED CONNECTED STATIC	nts one route. AD is	s the administrative dist Destination IP 64.101.0.0 172.22.1.0 10.250.250.0 10.200.159.0 0.0.0.0 Refresh	Ance. 255 255 0 255 255 0 255 255 255 248 0 0 0 0 0	Gateway 172 22 1.1 - - 10 250 250 1	Inter Inside Inside Dackup Outside Dackup	fed: 10/12/06 2:50:33 PM-
Data Refreshed	Successfully.					ck	100 2	🔂 🍰	6	10/12/06 2:49:42 PM UT

<u>トラブルシューティング</u>

<u>debug コマンド</u>

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 10.250.250.0 255.255.248 is directly connected, backup
- C 10.200.159.0 255.255.258 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 10.250.250.0 255.255.248 is directly connected, backup

C 10.200.159.0 255.255.248 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 10.250.250.0 255.255.248 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
	is unreachable so the route to the Primary ISP is removed

!--- 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。

<u>ASA での SLA モニタリング</u>

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

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