ループバック インターフェイス

この章では、ループバック インターフェイスを設定する方法について説明します。

ループバック インターフェイスについて

ループバック インターフェイスは、物理インターフェイスをエミュレートするソフトウェア専用インターフェイスであり、複数の物理インターフェイスを介して IPv4 および IPv6 に到達できます。ループバック インターフェイスはパス障害の克服に役立ちます。任意の物理インターフェイスからアクセスできるため、1 つがダウンした場合、別のインターフェイスからループバック インターフェイスにアクセスできます。

ループバック インターフェイスは、次の目的で使用できます。

- AAA
- BGP
- DNS
- HTTP
- ICMP
- SNMP
- SSH
- スタティックおよびダイナミック VTI トンネル
- Syslog
- Telnet

ASA は、ダイナミック ルーティング プロトコルを使用してループバックアドレスを配布できます。または、ピアデバイスでスタティックルートを設定して、 ASA のいずれかの物理インターフェイスを介してループバック IP アドレスに到達できます。ASA では、ループバック インターフェイスを指定するスタティックルートを設定できません。

ループバック インターフェイスの概要

フェールオーバー とクラスタリング

- クラスタリングはサポートされません。

コンテキスト モード

- VTIはシングルコンテキストモードでのみサポートされます。マルチコンテキストモードでは、他のループバックの使用がサポートされます。

その他のガイドラインと制限事項

- 物理インターフェイスからループバック インターフェイスへのトラフィックでは、TCP シーケンスのランダム化は常に無効になっています。

ループバック インターフェイスの設定

ループバック インターフェイスを追加します。

手順

ステップ 1 ループバック インターフェイスを作成します。

interface loopback *number*

0 ー 10413 の値を指定できます。

例：

```
ciscoasa(config)# interface loopback 10
```

ステップ 2 名前と IP アドレスを設定します。ルーテッド モードおよびトランスペアレント モードのインターフェイスを参照してください。

ステップ 3 ループバックトラフィックのレート制限を設定します。「ループバック インターフェイスへのトラフィックのレート制限 （3 ページ）」を参照してください。

ループバック インターフェイスへのトラフィックのレート制限

システムに過剰な負荷がかからないように、ループバック インターフェイス IP アドレスに送信されるトラフィックのレートを制限する必要があります。グローバルサービスポリシーに接続制限ルールを追加できます。この手順では、デフォルトのグローバルポリシー（global_policy）への追加を示します。

手順

ステップ 1 ループバック インターフェイス IP アドレスへのトラフィックを識別するアクセスリストを作成します。

access-list *name* **extended permit ip any host** *loopback_ip*

ループバック インターフェイス IP アドレスごとに ACE を作成します。**any** の代わりに送信元 IP アドレスを指定して、このアクセスリストを絞り込むこともできます。

例：

```
ciscoasa(config)# access-list loop extended permit ip any host 10.1.1.1
ciscoasa(config)# access-list loop extended permit ip any host 10.2.1.1
```

ステップ 2 アクセスリストを識別するクラスマップを作成します。

class-map *name*

match access-list *acl_name*

例：

```
ciscoasa(config)# class-map rate-limit-loopback
ciscoasa(config-cmap)# match access-list loop
```

ステップ 3 グローバルポリシーマップの一部として、最大接続数および最大初期接続数をクラスマップに適用します。

policy-map global_policy

class *class_map_name*

set connection conn-max *conns* **embryonic-conn-max** *conns*

最大接続数をループバック インターフェイスの予期される接続数に設定し、初期接続数をより低い数に設定します。予期される必要なループバック インターフェイス セッション数に応じて、たとえば、5/2、10/5、または 1024/512 に設定できます。

初期接続制限を設定するとTCP代行受信が有効になります。この代行受信によって、TCP SYNパケットを使用してインターフェイスをフラッディングするDoS攻撃からシステムを保護します。

例：

```
ciscoasa(config-cmap)# policy-map global_policy
ciscoasa(config-pmap)# class rate-limit-loopback
ciscoasa(config-pmap-c)# set connection conn-max 5 embryonic-conn-max 2
```

例

次の例では、2つのループバック インターフェイス（10.1.1.1と10.2.1.1）に送信されるすべてのトラフィックに適用されるデフォルトグローバルポリシーの最大接続数と初期接続数を10と5に設定します。

```
ciscoasa(config)# interface loopback 1
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# nameif loop1
ciscoasa(config-if)# interface loopback 2
ciscoasa(config-if)# ip address 10.2.1.1 255.255.255.0
ciscoasa(config-if)# nameif loop2
ciscoasa(config-if)# access-list loop extended permit ip any host 10.1.1.1
ciscoasa(config)# access-list loop extended permit ip any host 10.2.1.1
ciscoasa(config)# class-map CONNS
ciscoasa(config-cmap)# match access-list loop
ciscoasa(config-cmap)# policy-map global_policy
ciscoasa(config-pmap)# class CONNS
ciscoasa(config-pmap-c)# set connection conn-max 10 embryonic-conn-max 5
```

ループバック インターフェイスのモニタリング

次のコマンドを参照してください。

- **show interface**

  インターフェイス統計情報を表示します。

- **show interface ip brief**

  インターフェイスのIPアドレスとステータスを表示します。

ループバック インターフェイスの履歴

表 *1*: ループバック インターフェイスの履歴

機能名	バージョン	機能情報
DNS、HTTP、ICMP、IPsec フローオフロードのループバック インターフェイスのサポート	9.20(1)	ループバック インターフェイスを追加して、以下に使用できるようになりました。 • DNS • HTTP • ICMP • IPsec フローのオフロード
VTI のループバック インターフェイス サポート	9.19(1)	ループバック インターフェイスは、静的および動的 VTI VPN トンネルの冗長性を提供します。ループバック インターフェイスを VTI の送信元インターフェイスとして設定できるようになりました。VTI インターフェイスは、静的に設定された IP アドレスの代わりに、ループバック インターフェイスの IP アドレスを継承することもできます。ループバック インターフェイスは、パス障害の克服に役立ちます。インターフェイスがダウンした場合、ループバック インターフェイスの IP アドレスを使用してすべてのインターフェイスにアクセスできます。 新規/変更されたコマンド：**tunnel source interface**、**ip unnumbered**、**ipv6 unnumbered**
ループバック インターフェイスのサポート	9.18(2)	ループバック インターフェイスを追加して、以下に使用できるようになりました。 • BGP • AAA • SNMP • Syslog • SSH • Telnet 新規/変更されたコマンド：**interface loopback**、**logging host**、**neighbor update-source**、**snmp-server host**、**ssh**、**telnet**

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。