



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 \(1 ページ\)](#)
- [ループバック インターフェイスの概要 \(2 ページ\)](#)
- [ループバック インターフェイスの設定 \(2 ページ\)](#)
- [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 \(3 ページ\)](#)
- [ループバック インターフェイスの履歴 \(8 ページ\)](#)

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 [設定 (Configuration)] > [デバイス設定 (Device Setup)] > [インターフェイスの設定 (Interface Settings)] > [インターフェイス (Interfaces)] の順に選択します。

ステップ 2 [ループバック > インターフェイスの追加 (Add Loopback Interface)] を選択します。

[ループバックインターフェイスの追加 (Add Loopback Interface)] ダイアログボックスが表示されます。

ステップ 3 [ループバック ID (Loopback ID)] フィールドに、0 ~ 10413 の整数を入力します。

ステップ 4 インターフェイスがまだイネーブルでない場合は、[Enable Interface] チェックボックスをオンにします。

インターフェイスはデフォルトでイネーブルになっています。

ステップ 5 (任意) [説明 (Description)] フィールドに説明を入力します。

- ステップ 6** 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 7** [OK] をクリックします。
- [Interfaces] ペインに戻ります。
- ステップ 8** 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** [設定 (Configuration)] > [ファイアウォール (Firewall)] > [サービスポリシー (Service Policy)] を選択し、[追加 (Add)] > [サービスポリシー規則の追加 (Add Service Policy Rule)] をクリックします。
- ステップ 2** [グローバル (Global)] ポリシーを選択し、[次へ (Next)] をクリックします。

図 1: サービス ポリシー

Adding a new service policy rule requires three steps:

- Step 1: Configure a service policy.
- Step 2: Configure the traffic classification criteria for the service policy rule.
- Step 3: Configure actions on the traffic classified by the service policy rule.

Create a Service Policy and Apply To:

Only one service policy can be configured per interface or at global level. If a service policy already exists, then you can add a new rule into the existing service policy. Otherwise, you can create a new service policy.

☐ Interface: inside - (create new service policy) ⇅

Policy Name: inside-policy

Description:

☐ Drop and log unsupported IPv6 to IPv6 traffic

☒ Global - applies to all interfaces

Policy Name: global_policy *

Description:

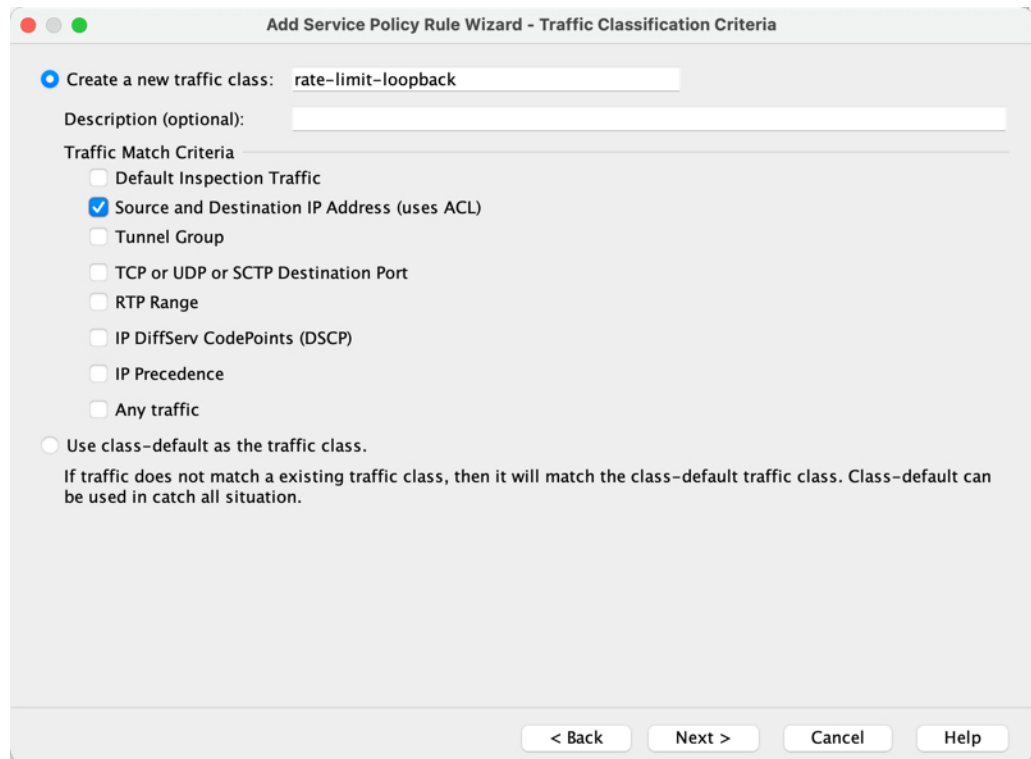
☐ Drop and log unsupported IPv6 to IPv6 traffic

*Only one service policy is allowed. Existing service policy names cannot be changed.

< Back Next > Cancel Help

ステップ 3 [トラフィック分類基準 (Traffic Classification Criteria)] ページで、次の値を設定して、[次へ (Next)] をクリックします。

図 2: トラフィック分類基準



- [新しいトラフィッククラスを作成（Create a new traffic class）]：ループバック トラフィック クラスに名前を付けます。
- [送信元および宛先IPアドレス（ACL を使用）（Source and Destination IP Address (uses ACL))]

ステップ 4 [トラフィックの一致：送信元および宛先アドレス（Traffic Match - Source and Destination Address）] ページで、ループバック IP アドレスに送信されるすべての IP トラフィックを指定するアクセス制御リストを定義し、[次へ（Next）] をクリックします。

図 3: [トラフィックの一致：送信元および宛先アドレス（**Traffic Match - Source and Destination Address**）]

Add Service Policy Rule Wizard - Traffic Match - Source and Destination Address

Action: ☒ Match ☐ Do not match

Existing ACL: ☐ ExistingACL

Source Criteria

Source: any

User:

Security Group:

Destination Criteria

Destination: loopback1, loopback2

Security Group:

Service: ip

Description:

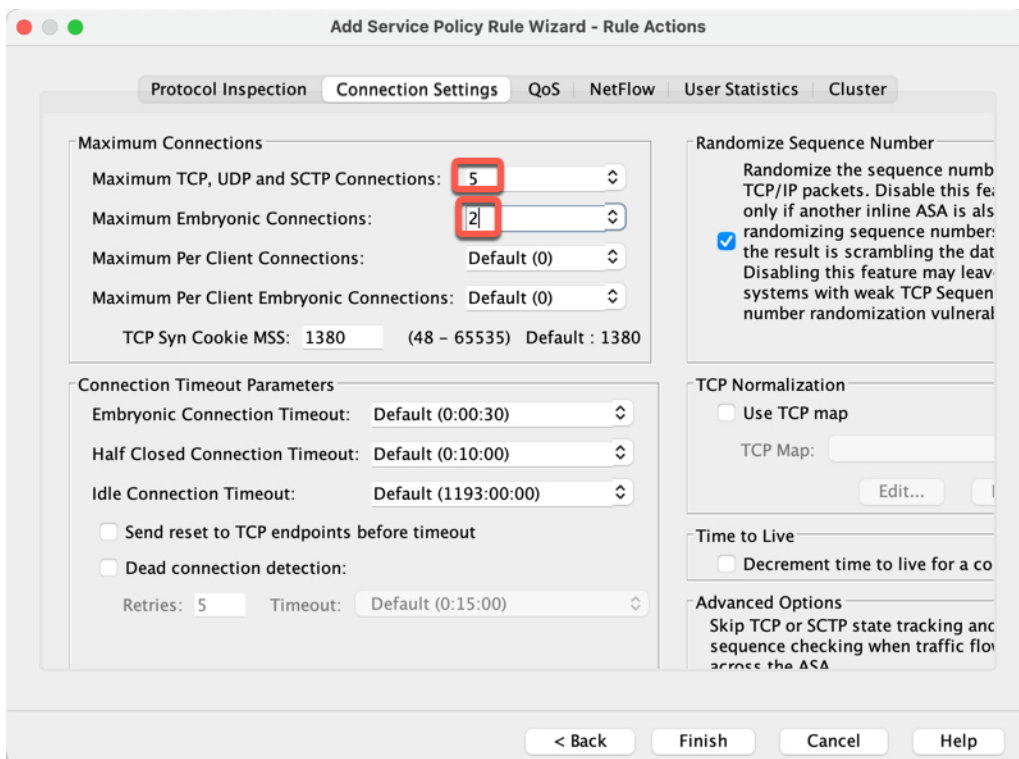
More Options

< Back Next > Cancel Help

- [アクション (Action)] : [一致 (Match)]
- [送信元 (Source)] : 「any」。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。
- [宛先 (Destination)] : ループバック インターフェイス IP アドレス
- [サービス (Service)] : 「ip」

ステップ 5 [規則アクション (Rule Actions)] ページで、[接続の設定 (Connection Settings)] タブをクリックし、[最大接続数 (Maximum Connections)] エリアで次の値を設定します。

図 4: 規則アクション



- [TCP、UDP、およびSCTPの最大接続数（Maximum TCP, UDP and SCTP Connections）]: 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。
- [初期接続数（Embryonic Connections）]: 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ディングする DoS 攻撃からシステムを保護します。

ステップ 6 [終了 (Finish)] をクリックします。

ルールがグローバルポリシーに追加されます。

図 5: サービス ポリシー ルール テーブル

Configuration > Firewall > Service Policy Rules										
Add Edit Delete Find Diagram Packet Trace										
Traffic Classification	Name	#	Enabled	Match	Source	Src Security Group	Destination	Dst Security Group	Service	Time
Global; Policy: global_policy	inspection_default			Match	any		any		default-in...	
	rate-limit-loopback	1	✓	Match	any		loopback1 loopback2		ip	
Rule Actions										
Inspect DNS Map p... Inspect ESMT... (12 more inspect actio... Max TCP/UDP Con... Max Embryonic Co...										

ステップ 7 [Apply] をクリックします。

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	920(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	919(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/変更された画面：[設定（Configuration）]>[デバイスのセットアップ（Device Setup）]>[インターフェイスの設定（Interface Settings）]>[インターフェイス（Interfaces）]>[VTI インターフェイスの追加（Add VTI Interface）]>[詳細（Advanced）]
ASDM でのループバック インターフェイスのサポート	919(1)	ASDM は、ループバック インターフェイスをサポートするようになりました。 新規/変更された画面：[設定（Configuration）]>[デバイスのセットアップ（Device Setup）]>[インターフェイスの設定（Interface Settings）]>[インターフェイス（Interfaces）]>[ループバック インターフェイスの追加（Add Loopback Interface）]

機能名	バージョン	機能情報
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 ASDM サポートはありません。

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。