

Interfaces de boucle avec retour

Ce chapitre explique comment configurer les interfaces de boucle avec retour.

- À propos des interfaces de boucle avec retour, à la page 1
- Directives pour les interfaces de boucle avec retour, à la page 2
- Configurer une interface de boucle avec retour, à la page 2
- Limite de débit du trafic vers l'interface de boucle avec retour, à la page 3
- Historique des interfaces de boucle avec retour, à la page 7

À propos des interfaces de boucle avec retour

Une interface de boucle avec retour est une interface logicielle uniquement qui émule une interface physique. Cette interface est accessible sur IPv4 et IPv6 par l'intermédiaire de plusieurs interfaces physiques. L'interface de boucle avec retour permet de résoudre les échecs de chemin. elle est accessible à partir de n'importe quelle interface physique. Par conséquent, si l'une d'elles tombe en panne, vous pouvez accéder à l'interface de boucle avec retour à partir d'une autre.

Les interfaces de boucle avec retour peuvent être utilisées pour :

- AAA
- BGP
- SNMP
- SSH
- Tunnels VTI statiques et dynamiques
- Syslog
- Telnet

L'ASA peut distribuer l'adresse de boucle avec retour à l'aide de protocoles de routage dynamique, ou vous pouvez configurer une voie de routage statique sur le périphérique homologue pour atteindre l'adresse IP de boucle avec retour par l'une des interfaces physiques de l'ASA. Vous ne pouvez pas configurer une voie de routage statique sur ASA qui spécifie l'interface de boucle avec retour.

Directives pour les interfaces de boucle avec retour

Basculement et mise en grappe

- Aucune prise en charge de mise en grappe.

Mode contextuel

- Le VTI est pris en charge en mode de contexte unique uniquement. Les autres utilisations de la boucle avec retour sont prises en charge en mode contexte multiple.

Directives et limites additionnelles

- La répartition aléatoire des séquences TCP est toujours désactivée pour le trafic de l'interface physique à l'interface de boucle avec retour.

Configurer une interface de boucle avec retour

Ajoutez une interface de boucle avec retour.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces**.

Étape 2 Choisissez **Add (Ajouter)** > **Loopback Interface (Interface de boucle avec retour)**.

La boîte de dialogue **Add Loopback Interface** (Ajouter une interface de boucle avec retour) s'affiche.

Étape 3 Dans le champ **Loopback ID** (ID de l'interface de boucle avec retour), saisissez un nombre entier entre 0 et 10413.

Étape 4 Si l'interface n'est pas déjà activée, cochez la case **Enable Interface** (Activer l'interface).

L'interface est activée par défaut.

Étape 5 (Facultatif) Saisissez une description dans le champ **Description**.

Étape 6 Configurez le nom et l'adresse IP. Consultez Interfaces en mode routage et en mode transparent

Étape 7 Cliquez sur **OK**.

Vous retournez dans le volet **Interfaces**.

Étape 8 Configurez la limitation de débit pour le trafic de boucle avec retour. Consultez Limite de débit du trafic vers l'interface de boucle avec retour, à la page 3.

Limite de débit du trafic vers l'interface de boucle avec retour

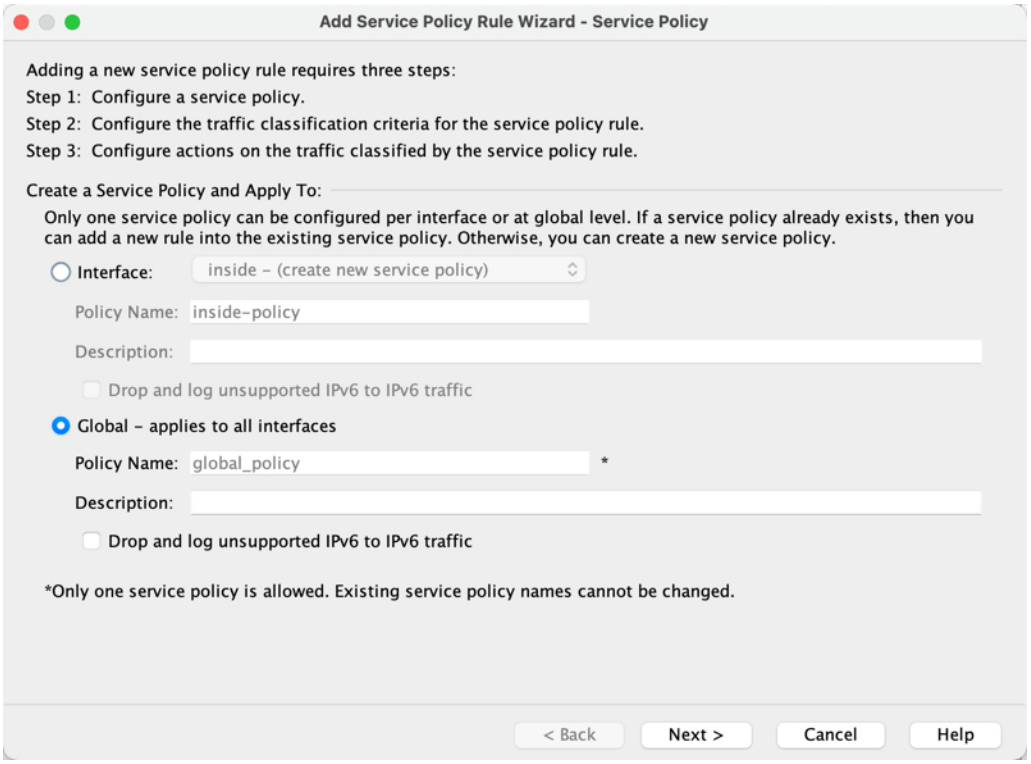
Vous devez limiter le trafic vers l'adresse IP de l'interface de boucle avec retour pour éviter une charge excessive sur le système. Vous pouvez ajouter une règle de limite de connexion à la politique de service globale. Cette procédure montre l'ajout à la politique globale par défaut (global_policy).

Procédure

Étape 1 Sélectionnez **Configuration** > **Firewall (Pare-feu)** > **Service Policy (Politique de service)**, puis cliquez sur **Add (Ajouter)** > **Add Service Policy Rule (Ajouter une règle de politique de service)**.

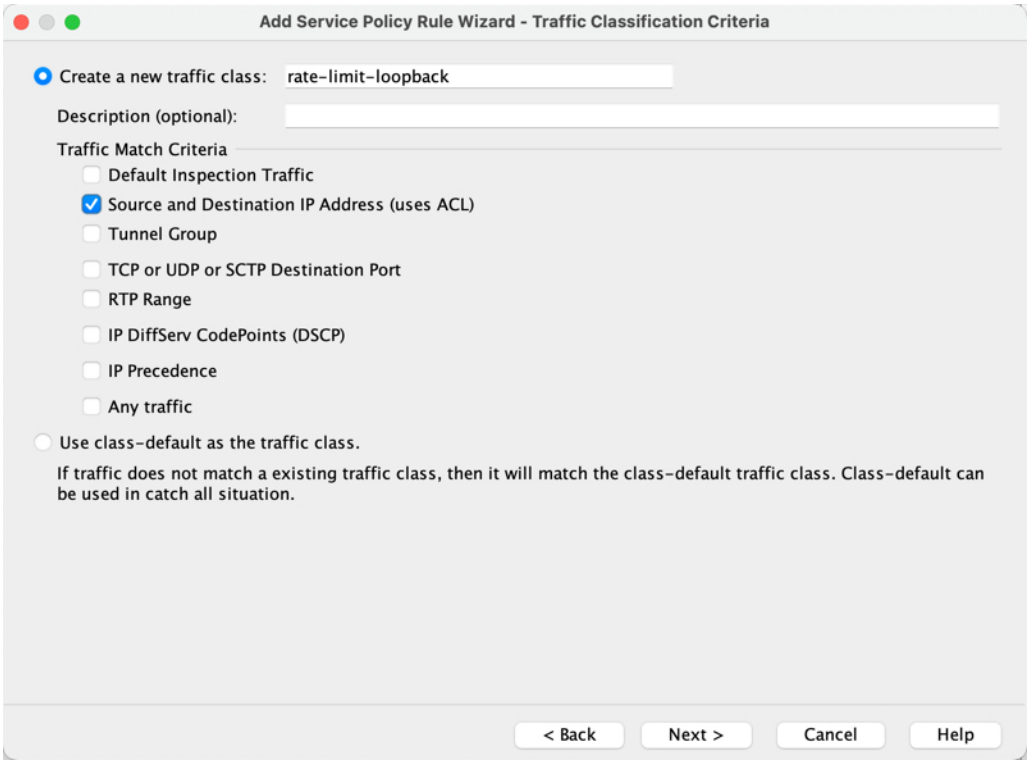
Étape 2 Sélectionnez la politique **Global** (Globale) et cliquez sur **Next** (Suivant).

Illustration 1 : Politique de service



Étape 3 Sur la page **Traffic Classification Criteria** (Critères de classification du trafic), définissez les valeurs suivantes et cliquez sur **Next** (Suivant).

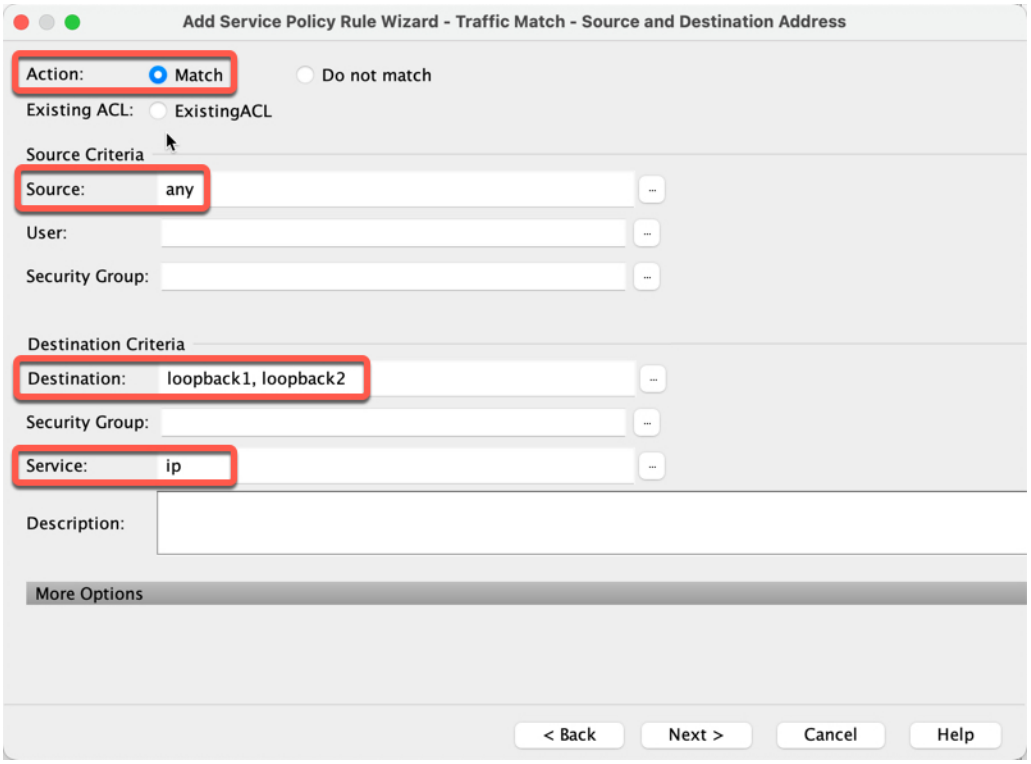
Illustration 2 : Critères de classification du trafic



- **Create a new traffic class** (Créer une nouvelle classe de trafic) : nommez la classe de trafic de boucle avec retour.
- **Source and Destination IP Address (uses ACL)** (Adresse IP source et de destination (utilise ACL))

Étape 4 Sur la page **Traffic Match - Source and Destination Address** (Concordance de trafic – Adresse source et de destination), définissez la liste de contrôle d'accès pour spécifier tout le trafic IP allant à l'adresse IP de boucle avec retour, puis cliquez sur **Next** (Suivant).

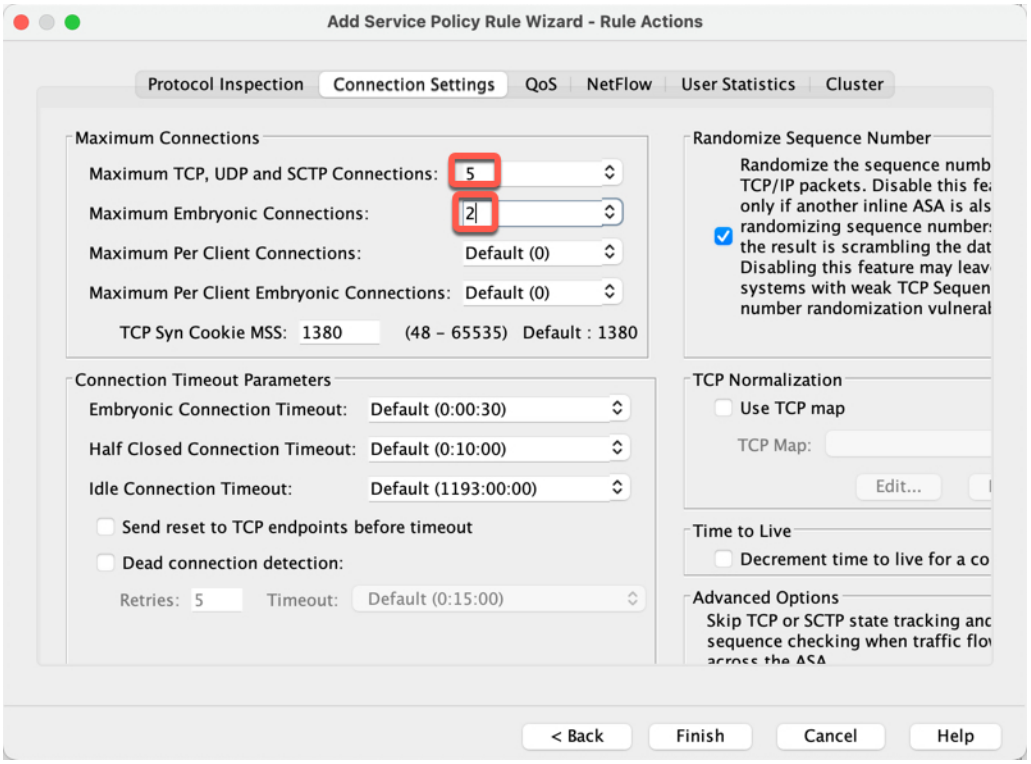
Illustration 3 : Correspondance de trafic – Adresse source et de destination



- **Action: Match** (Action : Mettre en correspondance)
- **Source** : toute. Vous pouvez également restreindre cette liste d'accès en spécifiant les adresses IP source plutôt que **any** (toute).
- **Destination** : les adresses IP de l'interface de boucle avec retour
- **Service** : ip

Étape 5 Sur la page **Rule Actions** (Actions découlant d'une règle), cliquez sur l'onglet **Connection Settings** (Paramètres de connexion) et dans la zone **Maximum Connections** (Nombre maximum de connexions), définissez les valeurs suivantes.

Illustration 4 : Actions découlant d'une règle

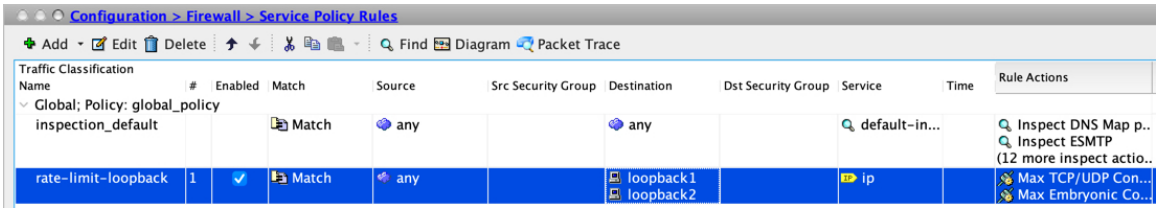


- **Maximum TCP, UDP and SCTP Connections** (Nombre maximum de connexions TCP, UDP et SCTP) : définissez le nombre maximum de connexions TCP et UDP sur le nombre attendu de connexions pour l'interface de boucle avec retour et le nombre de connexions amorces à un nombre inférieur. Par exemple, vous pouvez lui attribuer la valeur **5/2**, **10/5** ou **1024/512**, selon le nombre de sessions d'interface de boucle avec retour attendues dont vous avez besoin.
- **Embryonic Connections** (Connexions amorces) : la définition de la limite de connexions amorces active l'interception de TCP, qui protège le système contre une attaque DoS perpétrée en inondant une interface de paquets SYN de TCP.

Étape 6 Cliquez sur **Finish** (Terminer).

La règle est ajoutée à la politique globale.

Illustration 5 : Tableau des règles de politique de service



Étape 7 Cliquez sur **Apply** (Appliquer).

Historique des interfaces de boucle avec retour

Tableau 1 : Historique des interfaces de boucle avec retour

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
Prise en charge de l'interface de boucle avec retour pour VTI	9.19(1)	Une interface de boucle avec retour fournit la redondance des tunnels VPN VTI statiques et dynamiques. Vous pouvez désormais définir une interface de bouclage comme interface source pour un VTI. L'interface VTI peut également hériter de l'adresse IP d'une interface de boucle avec retour au lieu d'une adresse IP configurée de manière statique. L'interface de boucle avec retour permet de résoudre les échecs de chemin. Si une interface tombe en panne, vous pouvez accéder à toutes les interfaces grâce à l'adresse IP de l'interface de boucle avec retour. Écrans nouveaux/modifiés : **Configuration (configuration)** > **Device Setup (configuration de l'appareil)** > **Interface Settings (paramètres de l'interface)** > **Interfaces** > **Add VTI Interface (ajouter une interface VTI)** > **Advanced (avancé)**.
Prise en charge par ASDM des interfaces de bouclage	9.19(1)	ASDM prend désormais en charge les interfaces de bouclage. Écrans nouveaux/modifiés : **Configuration (configuration)** > **Device Setup (configuration de l'appareil)** > **Interface Settings (paramètres de l'interface)** > **Interfaces** > **Add Loopback Interface (ajouter une interface de bouclage)**.
Prise en charge de l'interface de boucle avec retour	9.18(2)	Vous pouvez maintenant ajouter une interface de boucle avec retour et l'utiliser pour : • BGP • AAA • SNMP • Journal système • SSH • Telnet Commandes nouvelles ou modifiées : **interface loopback**, **logging host**, **neighbor update-source**, **snmp-server host**, **ssh**, **telnet** ASDM n'est pas pris en charge.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.