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 2
- Supervision des interfaces de boucle avec retour, à la page 4
- Historique des interfaces de boucle avec retour, à la page 4

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

Le 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 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

Failover (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 Créez une interface de boucle avec retour :

interface loopback *number*

Le nombre peut être compris entre 0 et 10413.

Exemple :

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

Étape 2 Configurez le nom et l'adresse IP. Consultez Interfaces en mode routage et en mode transparent

Étape 3 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 2.

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 Créez une liste d'accès identifiant le trafic vers l'adresse IP de l'interface de boucle avec retour.

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

Créez un ACE pour chaque adresse IP d'interface de boucle avec retour. Vous pouvez également restreindre cette liste d'accès en spécifiant les adresses IP source plutôt que **any** (toute).

Exemple :

```
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
```

Étape 2 Créez une carte de trafic qui identifie la liste d'accès.

class-map *name*

match access-list *acl_name*

Exemple :

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

Étape 3 Appliquez le nombre maximum de connexions et de connexions amorces à la carte de trafic dans le cadre de la liste des politiques globales.

policy-map global_policy

class *class_map_name*

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

Définissez le nombre maximum de connexions 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 régler 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.

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.

Exemple :

```
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
```

Exemple

L'exemple suivant définit le nombre maximum de connexions et de connexions amorces à 10 et 5 pour la politique globale par défaut pour tout le trafic allant à deux interfaces de boucle avec retour à l'adresse 10.1.1.1 et 10.2.1.1.

```
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
```

Supervision des interfaces de boucle avec retour

Consultez les commandes suivantes :

- **show interface**

  Affiche des statistiques sur l'interface.

- **show interface ip brief**

  Affiche les adresses IP et l'état de l'interface.

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. Commandes nouvelles/modifiées : **tunnel source interface**, **ip unnumbered**, **ipv6 unnumbered**

Nom de la caractéristique	Version	Renseignements sur les fonctionnalités
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**

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.