

# Zones de circulation

Vous pouvez attribuer plusieurs interfaces à une *zone de trafic*, ce qui permet au trafic d'un flux existant de sortir ou d'entrer dans l'ASA sur n'importe quelle interface de la zone. Cette fonctionnalité permet le routage à chemins multiples à coûts égaux (ECMP) sur l'ASA, ainsi qu'à équilibrer la charge externe du trafic vers l'ASA sur plusieurs interfaces.


- À propos des zones de trafic, à la page 1
- Conditions préalables aux zones de trafic, à la page 7
- Lignes directrices relatives aux zones de trafic, à la page 9
- Configurer une zone de trafic, à la page 10
- Supervision des zones de trafic, à la page 11
- Exemple de zones de trafic, à la page 13
- Historique des zones de trafic, à la page 16


# À propos des zones de trafic

Cette section décrit comment vous devez utiliser les zones de trafic dans votre réseau.

## Comportement non zoné

L'algorithme de sécurité adaptatif prend en compte l'état d'un paquet lorsqu'il décide d'autoriser ou de refuser le trafic. L'un des paramètres appliqués pour le flux est que le trafic entre et sort de la même interface. Tout trafic pour un flux existant qui entre dans une interface différente est abandonné par l'ASA.

Les zones de trafic vous permettent de regrouper plusieurs interfaces afin que le trafic entrant ou sortant de *n'importe* quelle interface de la zone soit soumis aux contrôles de sécurité de l'algorithme de sécurité adaptatif.

**Sujets connexes**

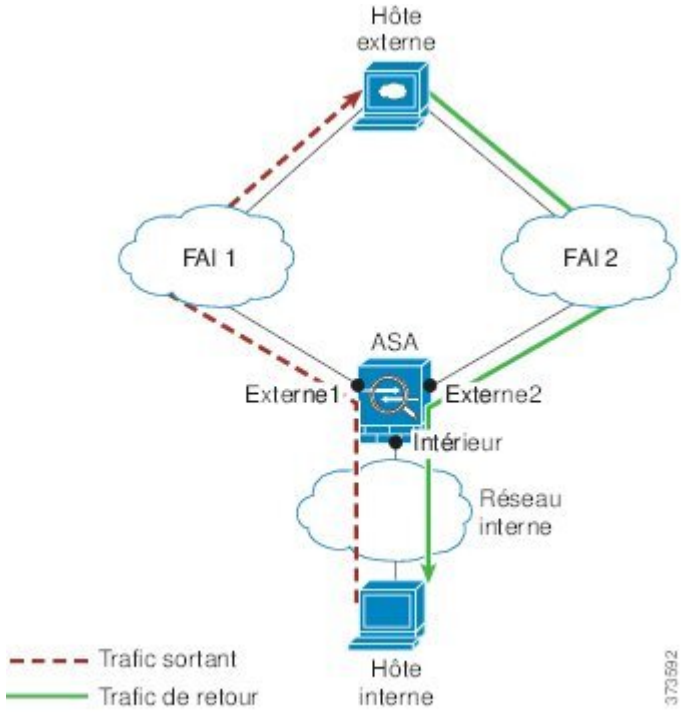
Présentation de l'inspection dynamique

## Pourquoi utiliser des zones?

Vous pouvez utiliser des zones pour vous servir de plusieurs scénarios de routage.

## Routage asymétrique

Dans le scénario suivant, une connexion a été établie entre un hôte interne et un hôte externe par le biais du FAI 1 sur l'interface Externe1. En raison d'un routage asymétrique sur le réseau de destination, le trafic de retour est arrivé du FAI 2 sur l'interface Externe2.

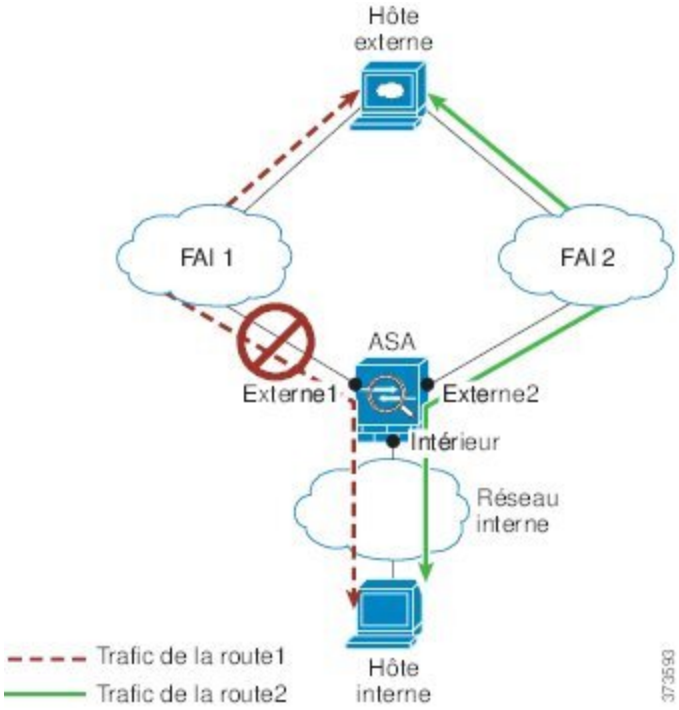



**Problème non zoné** : l'ASA gère les tables de connexion par interface. Lorsque le trafic de retour arrivera à Externe2, il ne correspondra pas à la table de connexion et sera abandonné. Pour une grappe ASA, le routage asymétrique lorsque la grappe a plusieurs contiguïtés avec le même routeur peut entraîner une perte de trafic inacceptable.

**Solution zonée** : l'ASA gère les tables de connexion par zone. Si vous regroupez Externe1 et Externe2 dans une zone, lorsque le trafic de retour arrivera à Externe2, il correspondra à la table de connexion par zone et la connexion sera autorisée.

## Route perdue

Dans le scénario suivant, une connexion a été établie entre un hôte interne et un hôte externe par le biais du FAI 1 sur l'interface Externe1. En raison d'une route perdue ou déplacée entre Externe1 et le FAI 1, le trafic doit emprunter une route différente par le FAI 2.

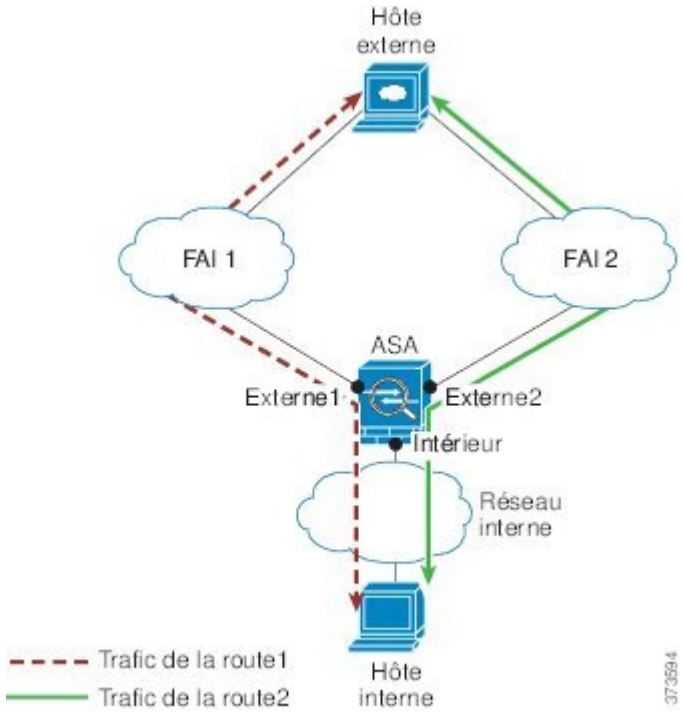



**Problème non zoné** : la connexion entre les hôtes interne et externe sera supprimée; une nouvelle connexion doit être établie à l'aide d'une nouvelle route optimale. Pour UDP, la nouvelle route sera utilisée après un seul abandon de paquet, mais pour TCP, une nouvelle connexion doit être rétablie.

**Solution zonée** : l'ASA détecte la route perdue et commute le flux dans le nouveau chemin par le biais du FAI 2. Le trafic sera transféré de manière transparente sans aucun abandon de paquets.

## Équilibrage de la charge

Dans le scénario suivant, une connexion a été établie entre un hôte interne et un hôte externe par le biais du FAI 1 sur l'interface Externe1. Une deuxième connexion a été établie par le biais d'une route à coût égal par le biais du FAI 2 sur l'interface Externe2.




**Problème non zoné** : l'équilibrage de charges sur les interfaces n'est pas possible; vous ne pouvez équilibrer la charge qu'avec des routes à coût égal sur une interface.

**Solution zonée** : l'ASA équilibre les connexions sur un maximum de huit routes à coût égal sur toutes les interfaces de la zone.

# Tables de connexion et de routage par zone

L'ASA gère une table de connexion par zone afin que le trafic puisse arriver sur n'importe quelle interface de zone. L'ASA gère également une table de routage par zone pour la prise en charge ECMP.

# Routage ECMP

L'ASA prend en charge le routage à chemins multiples à coûts égaux (ECMP).

## Prise en charge ECMP non zonée

Sans zones, vous pouvez avoir jusqu'à 8 routes statiques ou dynamiques de coût égal par interface. Par exemple, vous pouvez configurer trois routes par défaut sur l'interface externe qui spécifient différentes passerelles :

```
route outside 0 0 10.1.1.2
route outside 0 0 10.1.1.3
route outside 0 0 10.1.1.4
```

Dans ce cas, le trafic est équilibré en charge sur l'interface externe entre 10.1.1.2, 10.1.1.3 et 10.1.1.4. Le trafic est réparti entre les passerelles précisées selon un algorithme qui procède au hachage des adresses IP source et de destination, de l'interface entrante, du protocole et des ports source et destination.

Le protocole ECMP n'est pas pris en charge sur plusieurs interfaces; vous ne pouvez donc pas définir de route vers la même destination sur une interface différente. La route suivante n'est pas autorisée lorsqu'elle est configurée avec l'une des routes ci-dessus :

```
route outside2 0 0 10.2.1.1
```

## Prise en charge ECMP zonée

Avec les zones, vous pouvez avoir jusqu'à 8 voies de routage statiques ou dynamiques de coût égal sur 8 interfaces au maximum dans une zone.

Lorsque ECMP détermine la répartition du trafic, il voit chaque interface d'accès virtuelle comme un seul participant ou option de chemin, même si cette interface d'accès virtuelle est associée à une interface qui a plusieurs adresses IPv6.

Par exemple, vous pouvez configurer trois routes par défaut sur trois interfaces dans la zone :

```
route outside1 0 0 10.1.1.2
route outside2 0 0 10.2.1.2
route outside3 0 0 10.3.1.2
```

De même, votre protocole de routage dynamique peut configurer automatiquement des routes à coût égal. L'ASA équilibre la charge du trafic entre les interfaces grâce à un mécanisme d'équilibrage de la charge plus robuste.

Lorsqu'un routage est perdu, l'ASA déplace le flux de manière transparente vers une autre route.

## Équilibrage de charges des connexions

L'ASA équilibre la charge des connexions sur des routes à coût égal à l'aide d'un hachage effectué à partir du paquet à six tuples (adresses IP source et de destination, port de destination, protocole et interface d'entrée). À moins que la route ne soit perdue, une connexion restera sur l'interface choisie pendant sa durée.

Les paquets d'une connexion ne sont pas équilibrés en charge sur toutes les routes; une connexion utilise une seule route, sauf si cette route est perdue.

L'ASA ne prend pas en compte la bande passante de l'interface ni d'autres paramètres lors de l'équilibrage de charges. Vous devez vous assurer que toutes les interfaces de la même zone ont les mêmes caractéristiques telles que la MTU, la bande passante, etc.

L'algorithme d'équilibrage de charges n'est pas configurable par l'utilisateur.

## Basculement vers une route dans une autre zone

Lorsqu'une route est perdue sur une interface, s'il n'y a aucune autre route disponible dans la zone, l'ASA utilisera une route d'une interface ou d'une zone différente. Si cette route de secours est utilisée, vous pouvez rencontrer des abandons de paquet comme avec la prise en charge du routage non zoné.

# Politique de sécurité basée sur l'interface

Les zones permettent le trafic vers et en provenance de n'importe quelle interface de la zone, mais la politique de sécurité elle-même (critères d'accès, NAT, etc.) est toujours appliquée par interface et non par zone. Si vous configurez la même politique de sécurité pour toutes les interfaces de la zone, vous pouvez alors mettre

en œuvre avec succès l'ECMP et l'équilibrage de charges pour ce trafic. Pour en savoir plus sur la configuration d'interface parallèle requise, consultez Conditions préalables aux zones de trafic, à la page 7.

# Services pris en charge pour les zones de trafic

Les services suivants sont pris en charge avec les zones :

- Règles d'accès
- NAT
- Règles de service, à l'exception du contrôle de trafic QoS.
- Routage

Vous pouvez également configurer les services vers et à partir de la boîte répertoriés dans Trafic entrant et sortant, à la page 7, bien que la prise en charge complète des zones ne soit pas disponible.

Ne configurez pas d'autres services (comme le VPN ou le filtre de trafic de réseau de zombies) pour les interfaces dans une zone de trafic; elles peuvent ne pas fonctionner ou évoluer comme prévu.

**Remarque** Pour obtenir des renseignements détaillés sur la configuration de la politique de sécurité, consultez Conditions préalables aux zones de trafic, à la page 7.

# Niveaux de sécurité

La première interface que vous ajoutez à une zone détermine le niveau de sécurité de la zone. Toutes les interfaces supplémentaires doivent avoir le même niveau de sécurité. Pour modifier le niveau de sécurité des interfaces d'une zone, vous devez supprimer toutes les interfaces sauf une, puis modifier les niveaux de sécurité et rajouter les interfaces.

# Interface principale et actuelle pour le flux

Chaque flux de connexion est créé en fonction des interfaces d'entrée et de sortie initiales. Ces interfaces sont les interfaces *principales*.

Si une nouvelle interface de sortie est utilisée en raison de modifications de routes ou d'un routage asymétrique, les nouvelles interfaces sont les interfaces *actuelles*.

# Rejoindre ou quitter une zone

Lorsque vous affectez une interface à une zone, toutes les connexions sur cette interface sont supprimées. Les connexions doivent être rétablies.

Si vous supprimez une interface d'une zone, toutes les connexions qui ont l'interface comme interface principale sont supprimées. Les connexions doivent être rétablies. Si l'interface est l'interface actuelle, l'ASA ramène les connexions à l'interface principale. La table de routage de zone est également actualisée.

## Trafic intra-zone

Pour permettre au trafic d'*entrer* dans une interface et d'en *sortir*par une autre dans la même zone, activez **Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces > Enable traffic between two or more hosts connected to the same interface (Activer le trafic entre deux hôtes ou plus connectés à la même interface)**, qui permet au trafic d'entrer et de sortir de la même interface, ainsi que **Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces > Enable traffic between two or more interfaces which are configured with same security level (Activer le trafic entre deux interfaces ou plus qui sont configurées avec le même niveau de sécurité)**, qui autorise le trafic entre les interfaces de même sécurité. Sinon, un flux ne peut pas être acheminé entre deux interfaces dans la même zone.

## Trafic entrant et sortant

- Vous ne pouvez pas ajouter des interfaces de gestion uniquement ou d'accès de gestion à une zone.
- Pour le trafic de gestion sur les interfaces régulières d'une zone, seul le routage asymétrique sur les flux existants est pris en charge; il n'y a pas de prise en charge ECMP.
- Vous ne pouvez configurer un service de gestion que sur une seule interface de zone, mais pour profiter de la prise en charge du routage asymétrique, vous devez le configurer sur toutes les interfaces. Même lorsque les configurations sont parallèles sur toutes les interfaces, ECMP n'est pas pris en charge.
- L'ASA prend en charge les services entrant et sortant suivants dans une zone :
  - Telnet
  - SSH
  - HTTPS
  - SNMP
  - Journal système

## Chevauchement d'adresses IP dans une zone

Pour les interfaces non zonées, l'ASA prend en charge les réseaux d'adresses IP qui se chevauchent sur les interfaces tant que vous configurez la NAT correctement. Cependant, les réseaux qui se chevauchent ne sont pas pris en charge sur les interfaces de la même zone.

# Conditions préalables aux zones de trafic

- Configurez tous les paramètres d'interface, y compris le nom, l'adresse IP et le niveau de sécurité. Notez que le niveau de sécurité doit correspondre pour toutes les interfaces de la zone. Il est conseillé de regrouper les interfaces similaires en termes de bande passante et d'autres propriétés de couche 2.
- Configurez les services suivants pour qu'ils correspondent sur toutes les interfaces de zone :
  - Critères d'accès : appliquez le même critère d'accès à toutes les interfaces membres de la zone ou utilisez un critère d'accès global.

Par exemple :

```
access-list ZONE1 extended permit tcp any host WEBSERVER1 eq 80
access-group ZONE1 in interface outside1
access-group ZONE1 in interface outside2
access-group ZONE1 in interface outside3
```

- NAT : configurez la même politique NAT sur toutes les interfaces membres de la zone ou utilisez une règle NAT globale (en d'autres termes, utilisez « any » pour représenter les interfaces dans la règle NAT).

  L'interface PAT n'est pas prise en charge.

  Par exemple :

```
object network WEBSERVER1
  host 10.9.9.9 255.255.255.255
  nat (inside,any) static 209.165.201.9
```



**Remarque** Lorsque vous utilisez des ensembles NAT et PAT spécifiques à l'interface, l'ASA ne peut pas commuter les connexions en cas de défaillance de l'interface d'origine.

Si vous utilisez des ensembles PAT spécifiques à l'interface, plusieurs connexions du même hôte peuvent équilibrer la charge vers différentes interfaces et utiliser différentes adresses IP mappées. Les services Internet qui utilisent plusieurs connexions simultanées peuvent ne pas fonctionner correctement dans ce cas.

- Règles de service : utilisez la politique de service globale ou attribuez la même politique à chaque interface d'une zone.

  Le contrôle de trafic QoS n'est pas pris en charge.

  Par exemple :

```
service-policy outside_policy interface outside1
service-policy outside_policy interface outside2
service-policy outside_policy interface outside3
```

**Remarque** Pour les inspections VoIP, l'équilibrage de charges de la zone peut entraîner une augmentation des paquets désordonnés. Cette situation peut se produire, car les paquets ultérieurs peuvent atteindre l'ASA avant les paquets antérieurs qui empruntent un chemin différent. Les symptômes des paquets désordonnés sont les suivants :

- Utilisez la mémoire plus élevée aux nœuds intermédiaires (pare-feu et IDS) et aux nœuds de réception de la file d'attente si la mise en file d'attente est utilisée.
- Mauvaise qualité vidéo ou vocale.

Pour maîtriser ces effets, nous vous conseillons d'utiliser les adresses IP uniquement pour la répartition de la charge pour le trafic VoIP.

- Configurez le routage en tenant compte des capacités de la zone ECMP.

# Lignes directrices relatives aux zones de trafic

### Mode pare-feu

Pris en charge uniquement en mode de pare-feu routé. Ne prend pas en charge le mode de pare-feu transparent ni les interfaces de groupe de ponts en mode routé.

### Basculement

- Vous ne pouvez pas ajouter la liaison de basculement ou d'état à une zone.
- En mode de basculement actif/actif, vous pouvez attribuer une interface dans chaque contexte à un groupe de routage asymétrique (ASR). Ce service permet de restaurer le trafic renvoyé sur une interface similaire de l'unité homologue vers l'unité d'origine. Vous ne pouvez pas configurer à la fois des groupes ASR et des zones de trafic dans un contexte. Si vous configurez une zone dans un contexte, aucune des interfaces de contexte ne peut faire partie d'un groupe ASR. Consultez Configurer la prise en charge des paquets routés asymétriques (mode actif/actif) pour de plus amples renseignements sur les groupes ASR.
- Seules les interfaces principales de chaque connexion sont répliquées sur l'unité en veille; les interfaces actuelles ne sont pas répliquées. Si l'unité en veille devient active, elle attribuera une nouvelle interface actuelle, au besoin.

### Mise en grappe

- Vous ne pouvez pas ajouter la liaison de commande de grappe à une zone.

### Directives sur les modèles

Vous ne pouvez pas ajouter les ports de commutation ni les interfaces VLAN de Firepower 1010 à une zone.

### Directives supplémentaires

- Vous pouvez créer un maximum de 256 zones.
- Vous pouvez ajouter les types d'interfaces suivants à une zone :
  - Physique
  - VLAN
  - EtherChannel
- Vous ne pouvez pas ajouter les types d'interfaces suivants :
  - Gestion uniquement
  - Accès de gestion
  - Liaison de basculement ou d'état
  - Liaison de commande de la grappe
  - Interfaces membres dans un EtherChannel
  - VNI; de plus, si une interface de données standard est marquée comme nve-only, elle ne peut pas être membre d'une zone.
  - BVI ou interfaces membres d'un groupe de ponts.
- Une interface ne peut être membre que d'une seule zone.
- Vous pouvez inclure jusqu'à 8 interfaces par zone.
- Pour ECMP, vous pouvez ajouter jusqu'à 8 routes à coût égal par zone, sur toutes les interfaces de zone. Vous pouvez également configurer plusieurs routes sur une seule interface dans le cadre de la limite de 8 routes.
- Lorsque vous ajoutez une interface à une zone, toutes les routes statiques de ces interfaces sont supprimées.
- Vous ne pouvez pas activer le relais DHCP sur une interface dans une zone de trafic.
- L'ASA ne prend pas en charge le réassemblage des paquets fragmentés pour les fragments dont la charge est équilibrée sur des interfaces distinctes; ces fragments seront abandonnés.
- Le routage de multidiffusion PIM/IGMP n'est pas pris en charge sur les interfaces dans une zone.

# Configurer une zone de trafic

Configurez une zone nommée et affectez des interfaces à la zone.

### Procédure

**Étape 1** Choisissez**Configuration** > **Configuration du périphérique** > **Paramètres de l'interface** > **Zones**, et cliquez sur **Ajouter**.

Vous pouvez choisir d'affecter une interface à une zone à partir de la boîte de dialogue **Configuration > Configuration du périphérique > Paramètres d'interface > Interfaces > Ajouter une interface**.

**Étape 2** Le nom de la zone peut comporter jusqu'à 48 caractères.

**Étape 3** Ajouter une ou plusieurs interfaces à l'espace **membre**. Assurez-vous que toutes les interfaces ont le même niveau de sécurité.

**Étape 4** Cliquez sur **Apply** (Appliquer).

# Supervision des zones de trafic

Cette section décrit comment superviser les zones de trafic.

## Renseignements sur la zone

- **show zone** [*name*]

  Affiche l'ID de zone, le contexte, le niveau de sécurité et les membres.

  Consultez la sortie suivante pour la commande **show zone** :

```
ciscoasa# show zone outside-zone

Zone: zone-outside id: 2
Security-level: 0
Context: test-ctx
 Zone Member(s) : 2
  outside1       GigabitEthernet0/0
  outside2       GigabitEthernet0/1
```

- **show nameif zone**

  Affiche les noms d'interface et les noms de zone.

  Consultez la sortie suivante pour la commande **show nameif zone** :

```
ciscoasa# show nameif zone
Interface                Name                   zone-name      Security
GigabitEthernet0/0       inside-1               inside-zone     100
GigabitEthernet0/1.21    inside                 inside-zone     100
GigabitEthernet0/1.31    4                                        0
GigabitEthernet0/2       outside                outside-zone   0
Management0/0            lan                                      0
```

## Connexions de zone

- **show conn** [**long** | **detail**] [**zone** *zone_name* [**zone** *zone_name*] [...]]

  La commande **show conn zone** affiche les connexions pour une zone. Les mots clés **long** et **detail** affichent l'interface principale sur laquelle la connexion a été établie, et celle entre parenthèses est l'interface actuellement utilisée pour transférer le trafic ou l'interface d'où provient le dernier paquet.

Ainsi, l'interface actuelle, dans le cas d'une connexion provenant de plusieurs interfaces, peut afficher différentes interfaces à différents moments selon le moment où la commande show conn a été émise.

Consultez la sortie suivante pour la commande **show conn long zone** :

```
ciscoasa# show conn long zone zone-inside zone zone-outside

TCP outside-zone:outside1(outside2): 10.122.122.1:1080
inside-zone:inside1(inside2): 10.121.121.1:34254, idle 0:00:02, bytes 10, flags UO
```

- **show asp table zone**

  Affiche les tableaux de chemin de sécurité accélérés à des fins de débogage.

- **show local-host** [**zone** *zone_name* [**zone** *zone_name*] [...]]

  Affiche les états du réseau des hôtes locaux dans une zone.

  Consultez la sortie suivante pour la commande **show local-host zone**. L'interface principale est répertoriée en premier et l'interface actuelle est entre parenthèses.

```
ciscoasa# show local-host zone outside-zone

Zone:outside-zone: 4 active, 5 maximum active, 0 denied
local host: <10.122.122.1>,
    TCP flow count/limit = 3/unlimited
    TCP embryonic count to host = 0
    TCP intercept watermark = unlimited
    UDP flow count/limit = 0/unlimited

  Conn:
 TCP outside-zone:outside1(outside2): 10.122.122.1:1080
inside-zone:inside1(inside2): 10.121.121.1:34254, idle 0:00:02, bytes 10, flags UO
```

# Routage de zone

- **show route zone**

  Affiche les routes pour les interfaces de zone.

  Consultez la sortie suivante pour la commande **show route zone** :

```
ciscoasa# show route zone

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 not set

S    192.168.105.1 255.255.255.255 [1/0] via 172.16.1.1, outside-zone:outside1
C    192.168.212.0 255.255.255.0 is directly connected, lan-zone:inside,
C    172.16.1.0 255.255.255.0 is directly connected, wan-zone:outside2
S    10.5.5.0 255.255.255.0 [1/0] via 172.16.1.1, wan-zone:outside2
```

```
O    10.2.2.1 255.255.255.255 [110/11] via 192.168.212.3, 2:09:24, lan-zone:inside
O    10.1.1.1 255.255.255.255 [110/11] via 192.168.212.2, 2:09:24, lan-zone:inside
```

- **show asp table routing**

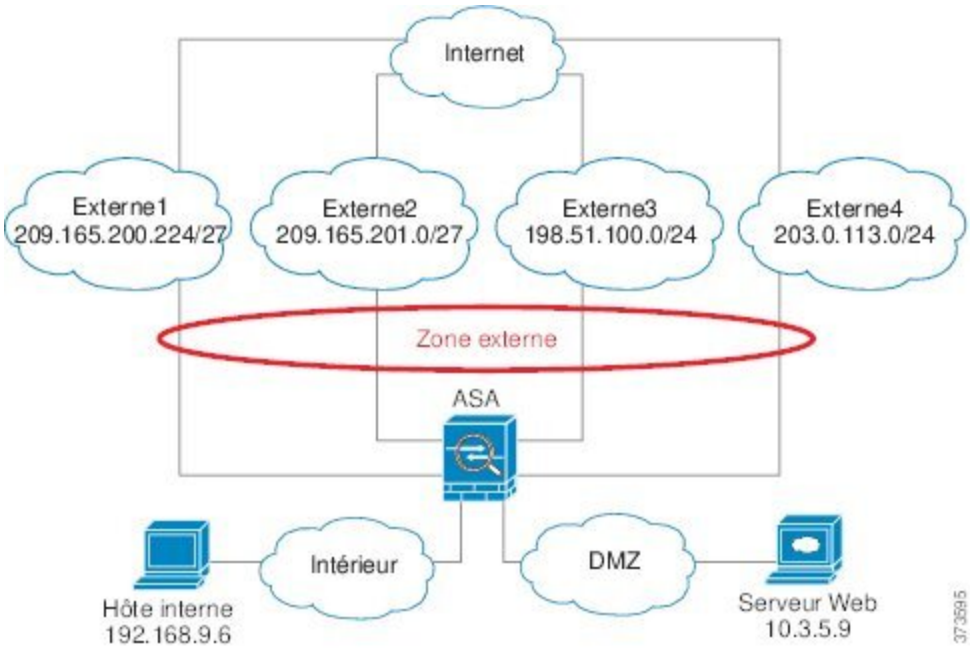
  Affiche les tableaux de chemins de sécurité accélérés à des fins de débogage et affiche la zone associée à chaque route.

  Consultez la sortie suivante pour la commande **show asp table routing** :

```
ciscoasa# show asp table routing
route table timestamp: 60
in   255.255.255.255 255.255.255.255 identity
in   10.1.0.1       255.255.255.255 identity
in   10.2.0.1       255.255.255.255 identity
in   10.6.6.4         255.255.255.255 identity
in   10.4.4.4         255.255.255.255 via 10.4.0.10 (unresolved, timestamp: 49)
in   172.0.0.67       255.255.255.255 identity
in   172.0.0.0       255.255.255.0   wan-zone:outside2
in   10.85.43.0      255.255.255.0   via 10.4.0.3 (unresolved, timestamp: 50)
in   10.85.45.0      255.255.255.0   via 10.4.0.20 (unresolved, timestamp: 51)
in   192.168.0.0        255.255.255.0   mgmt
in   192.168.1.0       255.255.0.0     lan-zone:inside
out  255.255.255.255 255.255.255.255 mgmt
out  172.0.0.67       255.255.255.255 mgmt
out  172.0.0.0        255.255.255.0   mgmt
out  10.4.0.0       240.0.0.0       mgmt
out  255.255.255.255 255.255.255.255 lan-zone:inside
out  10.1.0.1       255.255.255.255 lan-zone:inside
out  10.2.0.0       255.255.0.0     lan-zone:inside
out  10.4.0.0       240.0.0.0       lan-zone:inside
```

# Exemple de zones de trafic

L’exemple suivant affecte 4 interfaces VLAN à la zone externe et configure 4 routes par défaut à coût égal. La PAT est configurée pour l’interface interne, et un serveur Web est disponible sur une interface DMZ à l’aide de la NAT statique.




```
interface gigabitethernet0/0
  no shutdown
  description outside switch 1
interface gigabitethernet0/1
  no shutdown
  description outside switch 2

interface gigabitethernet0/2
  no shutdown
  description inside switch

zone outside

interface gigabitethernet0/0.101
  vlan 101
  nameif outside1
  security-level 0
  ip address 209.165.200.225 255.255.255.224
  zone-member outside
  no shutdown

interface gigabitethernet0/0.102
  vlan 102
  nameif outside2
  security-level 0
  ip address 209.165.201.1 255.255.255.224
  zone-member outside
  no shutdown

interface gigabitethernet0/1.201
  vlan 201
  nameif outside3
  security-level 0
  ip address 198.51.100.1 255.255.255.0
  zone-member outside
  no shutdown
```

```
interface gigabitethernet0/1.202
  vlan 202
  nameif outside4
  security-level 0
  ip address 203.0.113.1 255.255.255.0
  zone-member outside
  no shutdown

interface gigabitethernet0/2.301
  vlan 301
  nameif inside
  security-level 100
  ip address 192.168.9.1 255.255.255.0
  no shutdown

interface gigabitethernet0/2.302
  vlan 302
  nameif dmz
  security-level 50
  ip address 10.3.5.1 255.255.255.0
  no shutdown

# Static NAT for DMZ web server on any destination interface
object network WEBSERVER
  host 10.3.5.9 255.255.255.255
  nat (dmz,any) static 209.165.202.129 dns

# Dynamic PAT for inside network on any destination interface
object network INSIDE
  subnet 192.168.9.0 255.255.255.0
  nat (inside,any) dynamic 209.165.202.130

# Global access rule for DMZ web server
access-list WEB-SERVER extended permit tcp any host WEBSERVER eq 80
access-group WEB-SERVER global

# 4 equal cost default routes for outside interfaces
route outside1 0 0 209.165.200.230
route outside2 0 0 209.165.201.10
route outside3 0 0 198.51.100.99
route outside4 0 0 203.0.113.87
# Static routes for NAT addresses - see redistribute static command
route dmz 209.165.202.129 255.255.255.255 10.3.5.99
route inside 209.165.202.130 255.255.255.255 192.168.9.99

# The global service policy
class-map inspection_default
  match default-inspection-traffic
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum client auto
    message-length maximum 512
    dns-guard
    protocol-enforcement
    nat-rewrite
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225 _default_h323_map
    inspect h323 ras _default_h323_map
    inspect ip-options _default_ip_options_map
    inspect netbios
    inspect rsh
```

```
    inspect rtsp
    inspect skinny
    inspect esmtp _default_esmtp_map
    inspect sqlnet
    inspect sunrpc
    inspect tftp
    inspect sip
    inspect xdmcp
service-policy global_policy global
```

# Historique des zones de trafic

| Nom de la caractéristique | Versions de plateforme | Description |
|---|---|---|
| Zones de circulation | 9.3(2) | Vous pouvez regrouper les interfaces dans une zone de trafic pour réaliser l'équilibrage de la charge de trafic (à l'aide du routage ECMP (chemins multiples à coût égal)), la redondance de routes et le routage asymétrique sur plusieurs interfaces.<br>**Remarque**<br>Vous ne pouvez pas appliquer de politique de sécurité à une zone nommée; la politique de sécurité est basée sur l'interface. Lorsque les interfaces d'une zone sont configurées avec un critère d'accès, une NAT et une politique de service identiques, l'équilibrage de charges et le routage asymétrique fonctionnent correctement.<br>Nous avons introduit ou modifié les écrans suivants :<br>**Configuration > Device Setup (Configuration de l'appareil) > Interface Parameters (Paramètres d'interface) > Zones**<br>**Configuration > Device Setup (Configuration de l'appareil) > Interface Parameters (Paramètres d'interface) > Interfaces**. |
| commande **clear local-host** | 9.14(1) | La commande **clear local-host** et tous ses attributs et ses mots clés étaient obsolètes. Ils seront supprimés dans une version ultérieure. |

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.