

Mode pare-feu transparent ou routé

Ce chapitre décrit comment définir le mode du pare-feu routé ou transparent, ainsi que le fonctionnement du pare-feu dans chaque mode de pare-feu.

Vous pouvez définir le mode de pare-feu indépendamment pour chaque contexte en mode de contexte multiple.

- Mode pare-feu, à la page 1
- Paramètres de défaut, à la page 11
- Lignes directrices sur le mode pare-feu, à la page 11
- Définir le mode du pare-feu (mode unique), à la page 13
- Exemples de mode de pare-feu, à la page 14
- Historique du mode de pare-feu, à la page 25

Mode pare-feu

Un périphérique ASA prend en charge deux modes de pare-feu :

- Mode de pare-feu routé
- Mode de pare-feu transparent

Mode de pare-feu routé

En mode routage, l'ASA est considéré comme un saut de routeur dans le réseau. Chaque interface par laquelle vous souhaitez acheminer le trafic réseau se trouve sur un sous-réseau différent. Vous pouvez partager des interfaces de couche 3 entre les contextes.

Fonctionnalités intégrées de routage et de pontage

Avec le routage et le pont intégrés, vous pouvez utiliser un « groupe de ponts » dans lequel vous regroupez plusieurs interfaces sur un réseau, et l'ASA utilise des techniques de pont pour acheminer le trafic entre les interfaces. Chaque groupe de ponts comprend une interface virtuelle de pont (BVI) à laquelle vous attribuez une adresse IP sur le réseau. Les routes ASA entre les BVI et les interfaces de routage normales. Si vous n'avez pas besoin du mode à contextes multiples ou de mise en grappe, ni d'interfaces membres EtherChannel ou VNI, vous pouvez envisager d'utiliser le mode routé au lieu du mode transparent. En mode routé, vous pouvez avoir un ou plusieurs groupes de ponts isolés comme en mode transparent, mais vous pouvez également avoir des interfaces de routage normales pour un déploiement mixte.

Mode de pare-feu transparent

Classiquement, un pare-feu est un saut routé et agit comme une passerelle par défaut pour les hôtes qui se connectent à l'un de ses sous-réseaux filtrés. Un pare-feu transparent, en revanche, est un pare-feu de couche 2 qui agit comme une « présence sur le réseau câblé » ou un « pare-feu furtif », et qui n'est pas considéré comme un saut de routeur vers les appareils connectés. Cependant, comme tout autre pare-feu, le contrôle d'accès entre les interfaces est contrôlé et toutes les vérifications normales de pare-feu sont en place.

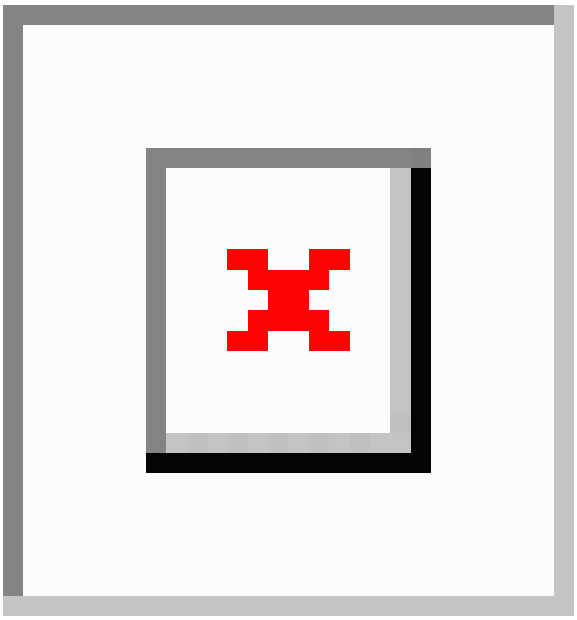
La connectivité de couche 2 est obtenue à l'aide d'un « groupe de ponts » où vous regroupez les interfaces interne et externe d'un réseau, où l'ASA utilise des techniques de pont pour acheminer le trafic entre les interfaces. Chaque groupe de ponts comprend une interface virtuelle de pont (BVI) à laquelle vous attribuez une adresse IP sur le réseau. Vous pouvez avoir plusieurs groupes de ponts pour plusieurs réseaux. En mode transparent, ces groupes de ponts ne peuvent pas communiquer entre eux.

Utilisation d'un réseau de pare-feu transparent

L'ASA relie le même réseau entre ses interfaces. Étant donné que le pare-feu n'est pas un tronçon de routage, vous pouvez facilement introduire un pare-feu transparent dans un réseau existant.

La figure suivante montre un réseau de pare-feu transparent typique où les périphériques externes se trouvent sur le même sous-réseau que les périphériques internes. Le routeur interne et les hôtes semblent être directement connectés au routeur externe.

Illustration 1 : Réseau de pare-feu transparent



Interface Management (gestion)

En plus de chaque adresse IP d'interface virtuelle de pont (BVI), vous pouvez ajouter une interface de Management (gestion) *logement*/*port* distincte qui ne fait partie d'aucun groupe de ponts et qui autorise uniquement le trafic de gestion vers l'ASA. Pour obtenir plus de renseignements, consultez Interface de gestion.

Passage de trafic pour les fonctionnalités en mode routé

Pour les fonctionnalités qui ne sont pas directement prises en charge sur le pare-feu transparent, vous pouvez laisser le trafic passer pour que les routeurs en amont et en aval prennent en charge la fonctionnalité.

Types de trafic pris en charge

Par exemple, en utilisant une règle d'accès, vous pouvez autoriser le trafic DHCP (au lieu de la fonction de relais DHCP non prise en charge) ou le trafic de multidiffusion comme celui créé par IP/TV. Vous pouvez également établir des contiguïtés de protocole de routage par l'intermédiaire d'un pare-feu transparent; vous pouvez autoriser le trafic OSPF, RIP, EIGRP ou BGP en fonction d'une règle d'accès. De même, des protocoles comme HSRP ou VRRP peuvent passer par l'ASA.

Groupes de ponts

Un groupe de ponts est un groupe d'interfaces que ASA relie par des ponts au lieu de routes. Les groupes de ponts sont pris en charge à la fois en mode transparent et en mode pare-feu routé. Comme toute autre interface de pare-feu, le contrôle d'accès entre les interfaces est contrôlé et toutes les vérifications normales de pare-feu sont en place.

Interfaces virtuelles de pont

Chaque groupe de ponts comprend une interface virtuelle de pont (BVI). ASA utilise l'adresse IP des BVI comme adresse source pour les paquets provenant du groupe de ponts. L'adresse IP BVI doit se trouver sur le même sous-réseau que les interfaces membres du groupe de ponts. Les BVI ne prennent pas en charge le trafic sur les réseaux secondaires; seul le trafic sur le même réseau que l'adresse IP BVI est pris en charge.

Fonctionnalité BVI par mode

En mode transparent : seules les interfaces des membres du groupe de ponts sont nommées et peuvent être utilisées avec les fonctionnalités basées sur l'interface.

En mode routé : les BVI servent de passerelle entre le groupe de ponts et les autres interfaces routées. Pour le routage entre groupes de ponts/interfaces routées, vous devez nommer le BVI. Pour certaines fonctionnalités basées sur l'interface, vous pouvez utiliser le BVI lui-même :

- Access Rules (règles d'accès) : vous pouvez configurer des règles d'accès pour les interfaces des membres des groupes de ponts et pour les BVI; pour les règles de trafic entrant, l'interface membre est vérifiée en premier. Pour les règles de trafic sortant, les BVI sont vérifiés en premier.
- Serveur DHCPv4 : seuls les BVI prennent en charge la configuration de serveur DHCPv4.
- Routes statiques : vous pouvez configurer des routes statiques pour les BVI; vous ne pouvez pas configurer de routage statique pour les interfaces membres.
- Serveur syslog et autre trafic provenant de l'ASA : lorsque vous spécifiez un serveur syslog (ou un serveur SNMP, ou un autre service où le trafic provient de l'ASA), vous pouvez spécifier une interface BVI ou une interface membre.

Si vous ne nommez pas les BVI en mode routé, ASA n'acheminera pas le trafic du groupe de ponts. Cette configuration reproduit le mode de pare-feu transparent pour le groupe de ponts. Si vous n'avez pas besoin du mode à contextes multiples ni de mise en grappe, ni d'interfaces membre EtherChannel ou VNI, vous pouvez envisager d'utiliser le mode routé à la place. En mode routé, vous pouvez avoir un ou plusieurs groupes

de ponts isolés comme en mode transparent, mais vous pouvez également avoir des interfaces de routage normales pour un déploiement mixte.

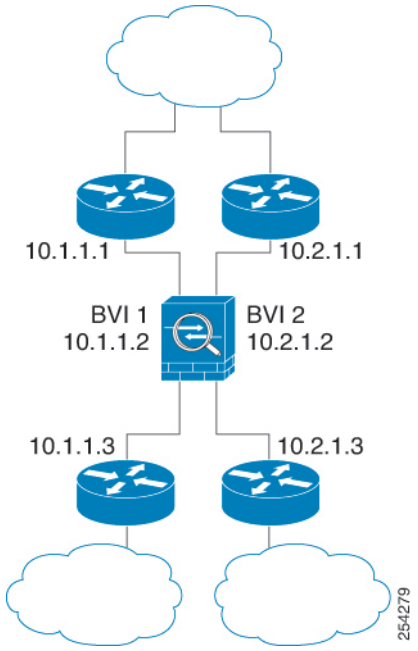
Groupes de ponts en mode pare-feu transparent

Le trafic des groupes de ponts est isolé des autres groupes de ponts; le trafic n'est pas acheminé vers un autre groupe de ponts dans ASA, et le trafic doit quitter ASA avant d'être acheminé par un routeur externe vers un autre groupe de ponts dans ASA. Bien que les fonctions de pont soient distinctes pour chaque groupe de ponts, de nombreuses autres fonctions sont partagées entre tous les groupes de ponts. Par exemple, tous les groupes de ponts partagent une configuration de serveur syslog ou de serveur AAA. Pour une séparation complète des politiques de sécurité, utilisez les contextes de sécurité avec un groupe de ponts dans chaque contexte.

Vous pouvez inclure plusieurs interfaces par groupe de ponts. Consultez Lignes directrices sur le mode pare-feu, à la page 11 pour connaître le nombre exact de groupes de ponts et d'interfaces pris en charge. Si vous utilisez plus de deux interfaces par groupe de ponts, vous pouvez contrôler la communication entre plusieurs segments du même réseau, et pas seulement entre l'intérieur et l'extérieur. Par exemple, s'il y a trois segments internes avec lesquels vous ne souhaitez pas communiquer, vous pouvez placer chaque segment sur une interface distincte et les autoriser uniquement à communiquer avec l'interface externe. Vous pouvez également personnaliser les règles d'accès entre les interfaces pour autoriser uniquement les accès souhaités.

La figure suivante montre deux réseaux connectés à un ASA, qui comporte deux groupes de ponts.

Illustration 2 : Réseau de pare-feu transparent avec deux groupes de ponts



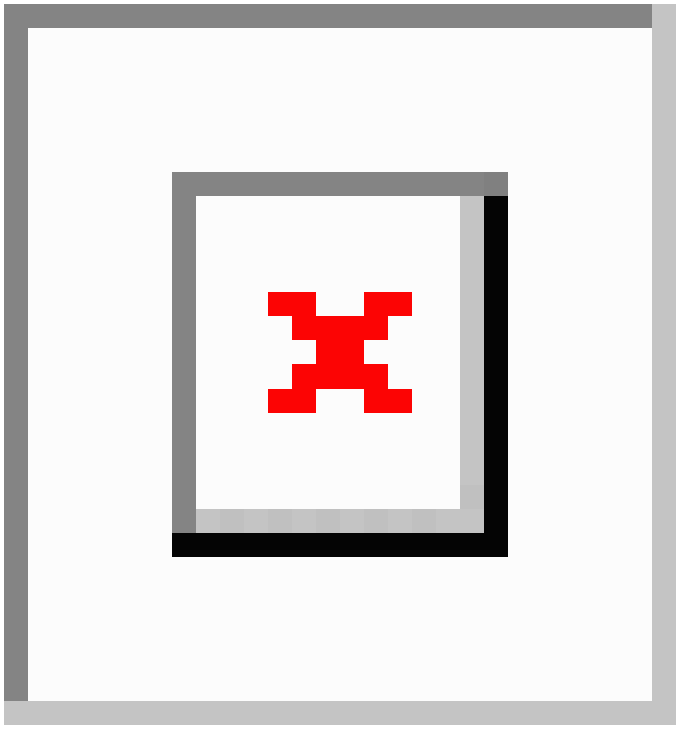
Groupes de ponts en mode pare-feu routé

Le trafic de groupe de ponts peut être acheminé vers d'autres groupes de ponts ou interfaces routées. Vous pouvez choisir d'isoler le trafic de groupe de ponts en n'attribuant pas de nom à l'interface BVI pour le groupe de ponts. Si vous nommez les BVI, alors les BVI participent au routage comme toute autre interface standard.

Utilisation et configuration du groupe de ponts

Une des utilisations d'un groupe de ponts en mode routé est d'utiliser des interfaces supplémentaires sur ASA au lieu d'un commutateur externe. Par exemple, la configuration par défaut de certains périphériques inclut une interface externe en tant qu'interface standard, puis toutes les autres interfaces affectées au groupe de ponts internes. Comme le but de ce groupe de ponts est de remplacer un commutateur externe, vous devez configurer une politique d'accès afin que toutes les interfaces du groupe de ponts puissent communiquer librement. Par exemple, comme dans la configuration par défaut, réglez toutes les interfaces au même niveau de sécurité, puis activez la communication de l'interface de même sécurité; aucune règle d'accès n'est requise.

Illustration 3 : Réseau de pare-feu routé avec un groupe de ponts interne et une interface routée externe



Transmission du trafic non autorisée en mode routé

En mode routé, certains types de trafic ne peuvent pas traverser l'ASA, même si vous l'autorisez dans un critère d'accès. Le groupe de ponts peut toutefois autoriser la quasi-totalité du trafic à passer en utilisant un critère d'accès (pour le trafic IP) ou une règle EtherType (pour le trafic non IP) :

- Trafic IP : en mode de pare-feu routé, le trafic de diffusion et de multidiffusion est bloqué même si vous l'autorisez dans un critère d'accès, y compris les protocoles de routage dynamique non pris en charge et le protocole DHCP (sauf si vous configurez le relais DHCP). Dans un groupe de ponts, vous pouvez autoriser ce trafic avec un critère d'accès.
- Trafic non IP : AppleTalk, IPX, BPDU et MPLS, par exemple, peuvent être configurés pour passer par une règle EtherType.

Remarque Le groupe de ponts ne transmet pas les paquets CDP ni les paquets qui n'ont pas d'EtherType valide supérieur ou égal à 0x600. Une exception est faite pour les BPDU et IS-IS, qui sont pris en charge.

Autorisation du trafic de couche 3

Cette rubrique décrit comment différents types de trafic de couche 3 sont traités par des groupes de ponts et les exigences des règles d'accès pour chaque type de trafic.

- Le trafic IPv4 et IPv6 de monodiffusion est autorisé par le groupe de ponts automatiquement d'une interface à sécurité supérieure vers une interface à sécurité inférieure, sans règle d'accès.
- Pour le trafic de couche 3 passant d'une interface de sécurité faible à une interface de sécurité élevée, une règle d'accès est requise sur l'interface de sécurité faible.
- Les protocoles ARP sont autorisés dans le groupe de ponts dans les deux sens sans règle d'accès. Le trafic ARP peut être contrôlé par inspection ARP.
- Les paquets de découverte de voisin IPv6 et de sollicitation de routeur peuvent être transmis à l'aide de règles d'accès.
- Le trafic en diffusion et en multidiffusion peut être transmis à l'aide de règles d'accès.

Adresses MAC autorisées

Les adresses MAC de destination suivantes sont autorisées par le biais du groupe de ponts si elles le sont par votre politique d'accès (voir Autorisation du trafic de couche 3, à la page 6). Toute adresse MAC qui ne figure pas dans cette liste est abandonnée.

- VRAIE adresse MAC de destination de diffusion égale à FFFF.FFFF.FFFF
- Adresses MAC IPv4 de multidiffusion, de 0100.5E00.0000 à 0100.5EFE.FFFF
- Adresses MAC IPv6 de multidiffusion, de 3333.0000.0000 à 3333.FFFF.FFFF
- Adresse de multidiffusion BPDU égale à 0100.0CCC.CCCD
- Adresses MAC AppleTalk de multidiffusion, de 0900.0700.0000 à 0900.07FF.FFFF

BPDU Handling (gestion des paquets BPDU)

Pour éviter les boucles avec le protocole Spanning Tree, les BPDU (Bridge Protocol Data Unit, Unité de données du protocole de pont) sont transmises par défaut. Pour bloquer les BPDU, vous devez configurer une règle EtherType pour les refuser. Vous pouvez également bloquer les BPDU sur les commutateurs externes. Par exemple, vous pouvez bloquer des BPDU sur le commutateur si des membres du même groupe de ponts sont connectés aux ports de commutation de différents VLAN. Dans ce cas, les BPDU d'un VLAN seront visibles dans l'autre VLAN, ce qui peut causer des problèmes de processus de sélection du pont racine du protocole Spanning Tree.

Si vous utilisez le basculement, vous souhaiterez peut-être bloquer les BPDU pour empêcher le port de commutation de passer à l'état de blocage lorsque la topologie change. Consultez Exigences en matière de groupes de ponts pour le basculement pour de plus amples renseignements.

Recherches d'adresse MAC ou de route

Pour le trafic à l'intérieur d'un groupe de ponts, l'interface sortante d'un paquet est déterminée en effectuant une recherche d'adresse MAC de destination plutôt qu'une recherche de route.

Cependant, les recherches de routage sont nécessaires dans les situations suivantes :

- Trafic provenant de l'ASA : ajoutez une voie de routage statique/par défaut sur l'ASA pour le trafic destiné à un réseau distant où se trouve un serveur syslog, par exemple.
- Politique SSL activée en mode de pare-feu transparent :
  - Le trafic TLS 1.3 passe par le périphérique ASA.
  - ASA agit en tant que proxy TCP. Il met fin à la connexion TCP du côté client et amorce une connexion distincte du côté du serveur. La pile TCP ASA est propriétaire de l'état de la session.
  - Pour les sessions proxy inactives, ASA génère des sondes Keepalive ACK du protocole TCP pour conserver l'état de la connexion. Il ne s'agit pas de paquets d'intercommunication : le pare-feu les crée et les envoie au client ou au serveur en fonction de l'état de la connexion de transit TLS.
  - Comme l'ASA est à l'origine de ces éléments Keepalives, il doit effectuer une recherche dans la table d'adjacence (résolution MAC de saut suivant ou de sortie) même en mode transparent.
  - Si la recherche d'adjacence échoue pour l'un de ces paquets générés par le proxy, l'ASA consigne le journal système 110003.

    Pour éviter ces messages syslog, configurez les routes sur l'ASA pour les points terminaux de la connexion de transit (adresses IP du client et du serveur). Un routage adéquat permet des recherches d'adjacence réussies pour les paquets Keepalive.

    Si l'ASA envoie un TCP Keepalive et reçoit une réponse, il maintient la connexion de transit active. Si le périphérique ne peut pas envoyer les Keepalives ou ne reçoit aucune réponse, il supprime la connexion de transit après environ 240 secondes.
- Trafic de voix sur IP (VoIP) et TFTP avec inspection activée, et le point terminal se trouve à au moins un saut (ajouter une route statique sur l'ASA pour le trafic destiné au point terminal distant afin que les connexions secondaires soient réussies. L'ASA crée un « trou » temporaire dans la politique de contrôle d'accès pour autoriser la connexion secondaire; et comme la connexion peut utiliser un ensemble d'adresses IP différent de celui de la connexion principale, l'ASA doit effectuer une recherche de routage pour installer le sténopé sur la bonne interface.

  Parmi les autres applications concernées, on trouve :
  - CTIQBE
  - GTP
  - H.323
  - MGCP
  - RTSP
  - SIP et Skinny (SCCP)
  - SQL*Net
  - SunRPC

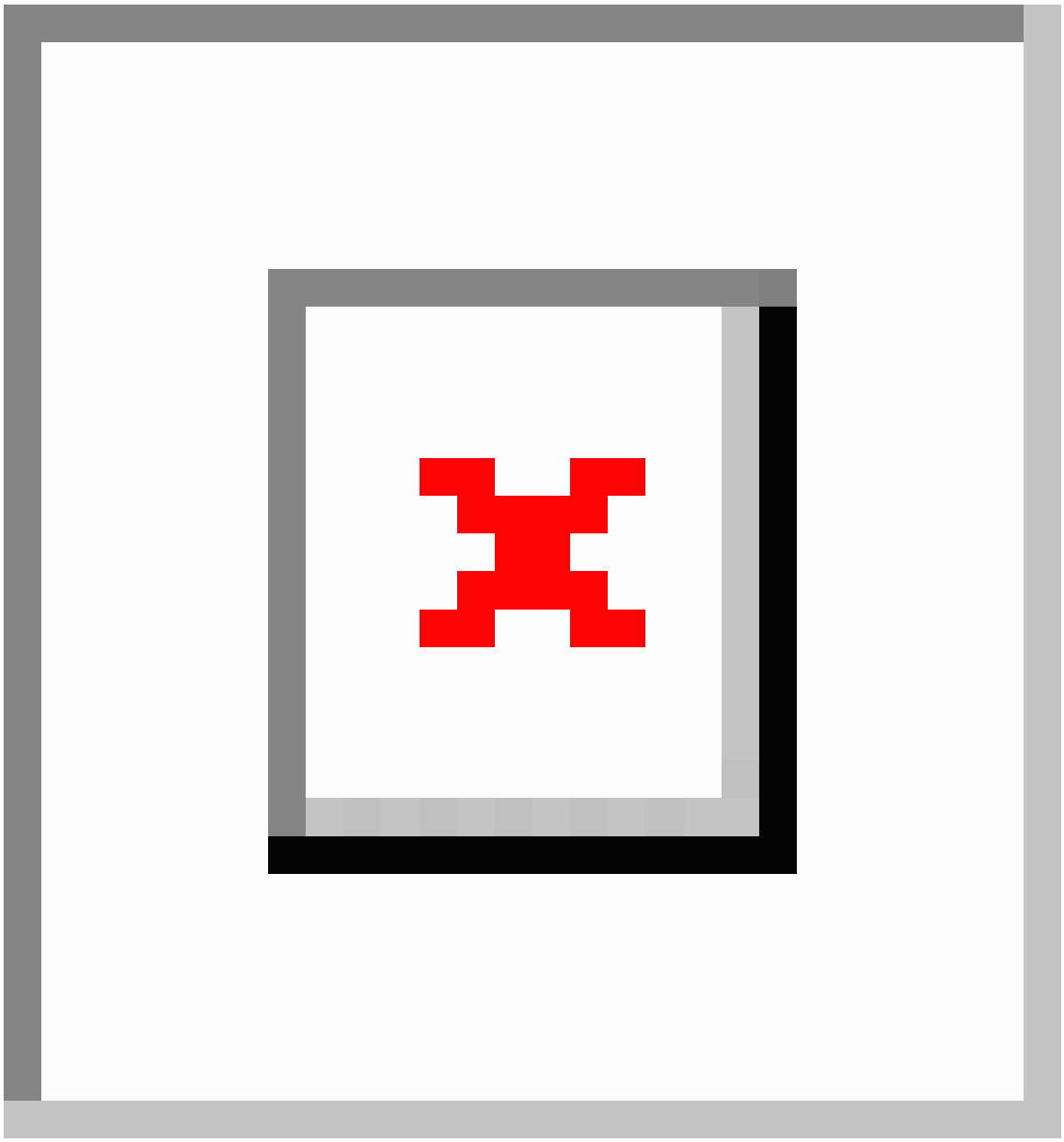
- TFTP

- Trafic à au moins un saut de distance pour lequel l'ASA exécute la NAT - Configurer une route statique sur l'ASA pour le trafic destiné au réseau distant. Vous avez également besoin d'une route statique sur le routeur en amont pour que le trafic destiné aux adresses mappées soit envoyé à l'ASA.

  Cette exigence de routage est également vraie pour les adresses IP intégrées pour VoIP et DNS avec inspection et NAT activées, et les adresses IP intégrées sont à au moins un sautillement. L'ASA doit identifier la bonne interface de sortie pour pouvoir effectuer la traduction.

NAT dans un groupe de pont

Illustration 4 : Exemple de NAT : NAT dans un groupe de pont



Fonctionnalités non prises en charge pour les groupes de ponts en mode transparent

Le tableau suivant répertorie les fonctionnalités non prises en charge dans les groupes de ponts en mode transparent.

Tableau 1 : Fonctionnalités non prises en charge en mode transparent

Fonctionnalités	Description
DNS dynamique	—
Serveur sans état DHCPv6	Seul le serveur DHCPv4 est pris en charge sur les interfaces membres des groupes de ponts.
Relais DHCP	Le pare-feu transparent peut servir de serveur DHCPv4, mais il ne prend pas en charge le relais DHCP. Le relais DHCP n'est pas nécessaire, car vous pouvez permettre au trafic DHCP de passer en utilisant deux règles d'accès : une qui autorise les requêtes DHCP de l'interface interne vers l'extérieur et une qui autorise les réponses du serveur dans l'autre sens.
Protocoles de routage dynamique	Vous pouvez, cependant, ajouter des routes statiques pour le trafic provenant des interfaces ASA pour les membres des groupes de ponts. Vous pouvez également autoriser les protocoles de routage dynamique à l'aide de l'ASA en utilisant une règle d'accès.
Routage de multidiffusion IP	Vous pouvez autoriser le trafic en multidiffusion via l'ASA en l'autorisant dans une règle d'accès.
Qualité de service	—
Terminaison VPN pour le trafic traversant	Le pare-feu transparent prend en charge les tunnels VPN de site à site pour les connexions de gestion uniquement sur les interfaces membres des groupes de ponts. Il ne met pas fin aux connexions VPN pour le trafic passant par ASA. Vous pouvez faire passer le trafic VPN par l'ASA à l'aide d'un critère d'accès, mais cela ne met pas fin aux connexions hors gestion.
Communications unifiées	—

Fonctionnalités non prises en charge pour les groupes de ponts en mode routé

Le tableau suivant répertorie les fonctionnalités non prises en charge dans les groupes de ponts en mode routé.

Tableau 2 : Fonctionnalités non prises en charge en mode routé

Fonctionnalités	Description
Interfaces membre EtherChannel ou VNI	Seules les interfaces physiques et les sous-interfaces sont prises en charge en tant qu'interfaces de membres de groupes de ponts. Les interfaces Management (gestion) ne sont pas non plus prises en charge.
Mise en grappe	Les groupes de ponts ne sont pas pris en charge dans la mise en grappe.
DNS dynamique	—
Serveur sans état DHCPv6	Seul le serveur DHCPv4 est pris en charge sur les BVI.

Fonctionnalités	Description
Relais DHCP	Le pare-feu routé peut servir de serveur DHCPv4, mais il ne prend pas en charge le relais DHCP sur les BVI ou les interfaces membres de groupes de ponts.
Protocoles de routage dynamique	Vous pouvez, cependant, ajouter des routes statiques pour les BVI. Vous pouvez également autoriser les protocoles de routage dynamique à l'aide de l'ASA en utilisant une règle d'accès. Les interfaces de groupe sans pont prennent en charge le routage dynamique.
Routage de multidiffusion IP	Vous pouvez autoriser le trafic en multidiffusion via l'ASA en l'autorisant dans une règle d'accès. Les interfaces de groupe sans pont prennent en charge le routage de multidiffusion.
Mode contexte multiple	Les groupes de ponts ne sont pas pris en charge en mode contexte multiple.
Qualité de service	Les interfaces sans groupe de ponts prennent en charge la QoS.
Terminaison VPN pour le trafic traversant	Vous ne pouvez pas mettre fin à une connexion VPN sur les BVI. Les interfaces qui ne font pas partie d'un groupe de pont prennent en charge le VPN. Les interfaces membres des groupes de ponts prennent en charge les tunnels VPN de site à site pour les connexions de gestion uniquement. Il ne met pas fin aux connexions VPN pour le trafic passant par ASA. Vous pouvez faire passer le trafic VPN par le groupe de ponts à l'aide d'une règle d'accès, mais cela ne met pas fin aux connexions hors gestion. Le VPN SSL sans client n'est pas non plus pris en charge.
Communications unifiées	Les interfaces de groupe hors pont prennent en charge les communications unifiées.

Paramètres de défaut

Répertorie les paramètres par défaut pour le mode de pare-feu.

Mode par défaut

Le mode par défaut est le mode routé.

Valeurs par défaut des groupes de ponts

Par défaut, tous les paquets ARP sont transmis au sein du groupe de ponts.

Lignes directrices sur le mode pare-feu

Passez en revue ces lignes directrices relatives au mode de pare-feu.

Lignes directrices relatives au mode contextuel

Définissez le mode de pare-feu par contexte.

Limites de groupe de ponts et exigences de réseau

- Chaque réseau connecté directement doit se trouver sur le même sous-réseau.
- Le périphérique de pare-feu Threat Defense ne prend pas en charge le trafic sur les réseaux secondaires ; seul le trafic sur le même réseau que l'adresse IP BVI est pris en charge.

Exigences relatives à l'adresse IP BVI

- Une adresse IP pour le BVI est requise pour chaque groupe de ponts pour le trafic de gestion vers le périphérique et en provenance du périphérique, ainsi que pour le trafic de données qui doit passer par le périphérique de pare-feu Threat Defense. Pour le trafic IPv4, spécifiez une adresse IPv4. Pour le trafic IPv6, spécifiez une adresse IPv6.
- Vous ne pouvez configurer les adresses IPv6 que manuellement.
- L'adresse IP BVI doit se trouver sur le même sous-réseau que le réseau connecté. Vous ne pouvez pas définir le sous-réseau comme sous-réseau d'hôte (255.255.255.255).

Membres du groupe de ponts non pris en charge

- Les interfaces de gestion ne sont pas prises en charge en tant que membres de groupes de ponts.
- Pour l'ASAv50 sur VMware avec des interfaces ixgbevf pontées, le mode transparent n'est pas pris en charge et les groupes de ponts ne sont pas pris en charge en mode routé.
- Pour Série Firepower 2100, les groupes de ponts ne sont pas pris en charge en mode routé.
- Pour le 200/ 1010/ , il n'est pas possible de mélanger des interfaces VLAN logiques et des interfaces de pare-feu physiques au sein du même groupe de ponts.

Exigences et limites du mode transparent

- En mode transparent, vous devez utiliser au moins un groupe de ponts; les interfaces de données doivent appartenir à un groupe de ponts.
- En mode transparent, ne spécifiez pas l'adresse IP des BVI comme passerelle par défaut pour les périphériques connectés; Les périphériques doivent spécifier le routeur de l'autre côté de la ASA comme passerelle par défaut.
- En mode transparent, la voie de routage par défaut, qui est requise pour fournir un chemin de retour au trafic de gestion, n'est appliquée qu'au trafic de gestion provenant d'un réseau de groupe de ponts. En effet, la voie de routage par défaut spécifie une interface dans le groupe de ponts ainsi que l'adresse IP du routeur sur le réseau du groupe de ponts, et vous ne pouvez définir qu'une seule voie de routage par défaut. Si votre trafic de gestion provient de plus d'un réseau de groupes de ponts, vous devez spécifier une voie de routage statique régulière qui identifie le réseau à partir duquel vous attendez le trafic de gestion.
- Le protocole PPPoE n'est pas pris en charge sur l'interface Management (gestion).

Exigences et limites du mode routé

- En mode routé, pour le routage entre les groupes de ponts et les autres interfaces routées, vous devez nommer les BVI.
- En mode routé, les interfaces EtherChannel définies par ASA et VNI ne sont pas prises en charge en tant que membres de groupes de ponts. Les EtherChannels sur Firepower 4100/9300 peuvent être des membres de groupes de ponts.

Limitation relative au traitement du trafic

- Les paquets écho de la détection de transfert bidirectionnel (BFD) ne sont pas autorisés par le biais de l'ASA lors de l'utilisation de membres de groupe de ponts. S'il y a deux voisins de chaque côté de l'ASA exécutant BFD, alors l'ASA abandonnera les paquets écho BFD, car ils ont la même adresse IP de source et de destination et semblent faire partie d'une attaque LAND.

Définir le mode du pare-feu (mode unique)

Cette section décrit comment changer de mode de pare-feu à l'aide de la CLI. Pour le mode unique et pour le contexte actuellement connecté en mode multiple (généralement le contexte d'administration), vous ne pouvez pas modifier le mode dans ASDM. Pour les autres contextes de modes multiples, vous pouvez définir le mode dans ASDM pour chaque contexte; voir Configurer un contexte de sécurité.

Remarque Nous vous recommandons de définir le mode de pare-feu avant d'effectuer toute autre configuration, car la modification de ce dernier efface la configuration en cours.

Avant de commencer

Lorsque vous changez de mode, l'ASA efface la configuration en cours (voir Lignes directrices sur le mode pare-feu, à la page 11 pour plus d'informations).

- Si vous avez déjà une configuration remplie, assurez-vous de sauvegarder votre configuration avant de modifier le mode. vous pouvez utiliser cette sauvegarde comme référence lors de la création de votre nouvelle configuration.
- Utilisez l'interface de ligne de commande du port de console pour changer de mode. Si vous utilisez tout autre type de session, y compris l'outil de l'interface de ligne de commande ASDM ou SSH, vous serez déconnecté lorsque la configuration sera effacée et vous devrez vous reconnecter à l'ASA en utilisant le port de console dans tous les cas.
- Définissez le mode dans le contexte.

Remarque Pour définir le mode de pare-feu à transparent et également configurer l'accès de gestion ASDM après avoir effacé la configuration, consultez Configurer l'accès ASDM.

Procédure

Définissez le mode de pare-feu sur transparent :

Pare-feu transparent

Exemple :

```
ciscoasa(config)# firewall transparent
```

Pour changer le mode à routé, saisissez la commande **no firewall transparent** (pas de pare-feu transparent).

Remarque Vous n'êtes pas invité à confirmer le changement de mode de pare-feu; la modification se produit immédiatement.

Exemples de mode de pare-feu

Cette section comprend des exemples illustrant la manière dont le trafic circule à travers l'ASA en mode de pare-feu routé et transparent.

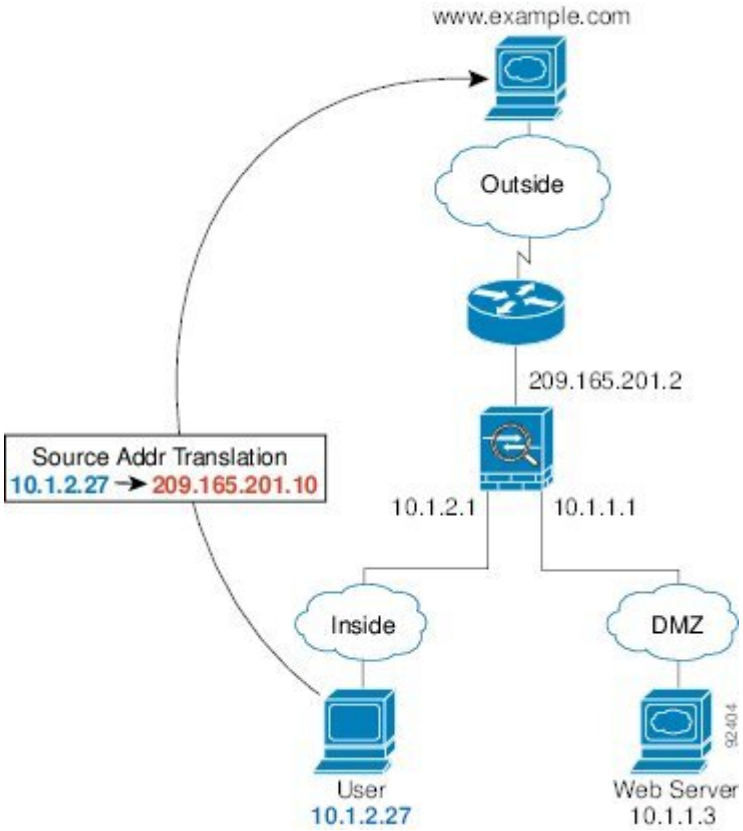
Progression des données dans l'ASA en mode de pare-feu routé

Les sections suivantes décrivent comment les données passent par l'ASA en mode de pare-feu routé dans plusieurs scénarios.

Un utilisateur interne visite un serveur web

La figure suivante montre un utilisateur interne accédant à un serveur web externe.

Illustration 5 : De l'intérieur vers l'extérieur



Les étapes suivantes décrivent comment les données passent par l'ASA :

1. L'utilisateur sur le réseau interne demande une page Web à www.exemple.com.
2. L'ASA reçoit le paquet et, comme il s'agit d'une nouvelle session, il vérifie que le paquet est autorisé selon les conditions de la politique de sécurité.

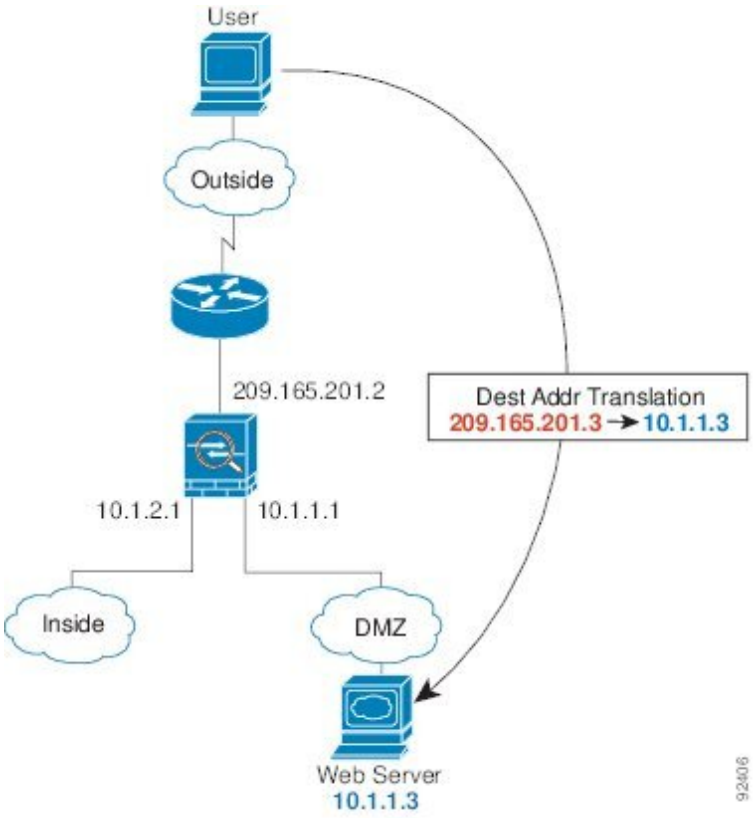
   Pour le mode de contexte multiple, l'ASA classe d'abord le paquet dans un contexte.
3. L'ASA traduit l'adresse réelle (10.1.2.27) en adresse mappée 209.165.201.10, qui se trouve sur le sous-réseau de l'interface externe.

   L'adresse mappée peut se trouver sur n'importe quel sous-réseau, mais le routage est simplifié lorsqu'elle se trouve sur le sous-réseau d'interface externe.
4. L'ASA enregistre ensuite qu'une session est établie et transfère le paquet de l'interface externe.
5. Lorsque www.exemple.com répond à la demande, le paquet passe par l'ASA, et comme la session est déjà établie, le paquet contourne les nombreuses recherches associées à une nouvelle connexion. L'ASA effectue la NAT en ne traduisant pas l'adresse de destination globale en adresse d'utilisateur locale, 10.1.2.27.
6. L'ASA transmet le paquet à l'utilisateur interne.

Un utilisateur externe visite un serveur web sur la DMZ

La figure suivante montre un utilisateur externe accédant au serveur web DMZ.

Illustration 6 : Externe vers DMZ



Les étapes suivantes décrivent comment les données passent par l'ASA :

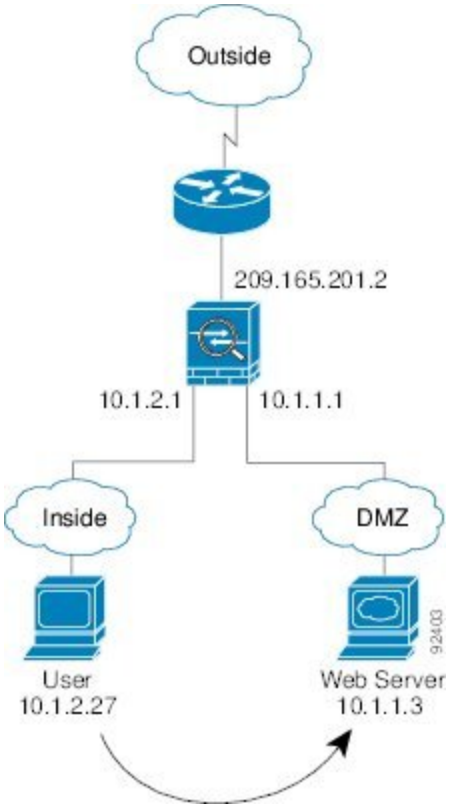
1. Un utilisateur sur le réseau externe demande une page Web au serveur web DMZ en utilisant l'adresse mappée 209.165.201.3, qui se trouve sur le sous-réseau de l'interface externe.
2. L'ASA reçoit le paquet et traduit l'adresse mappée en adresse réelle 10.1.1.3.
3. Comme il s'agit d'une nouvelle session, l'ASA vérifie que le paquet est autorisé selon les conditions de la politique de sécurité.

   Pour le mode de contexte multiple, l'ASA classe d'abord le paquet dans un contexte.
4. L'ASA ajoute ensuite une entrée de session au chemin rapide et transfère le paquet de l'interface DMZ.
5. Lorsque le serveur web DMZ répond à la demande, le paquet passe par l'ASA et, comme la session est déjà établie, le paquet contourne les nombreuses recherches associées à une nouvelle connexion. L'ASA effectue la NAT en traduisant l'adresse réelle en 209.165.201.3.
6. L'ASA transmet le paquet à l'utilisateur externe.

Un utilisateur interne visite un serveur web sur la DMZ

La figure suivante montre un utilisateur interne accédant au serveur web DMZ.

Illustration 7 : Interne à DMZ



Les étapes suivantes décrivent comment les données passent par l'ASA :

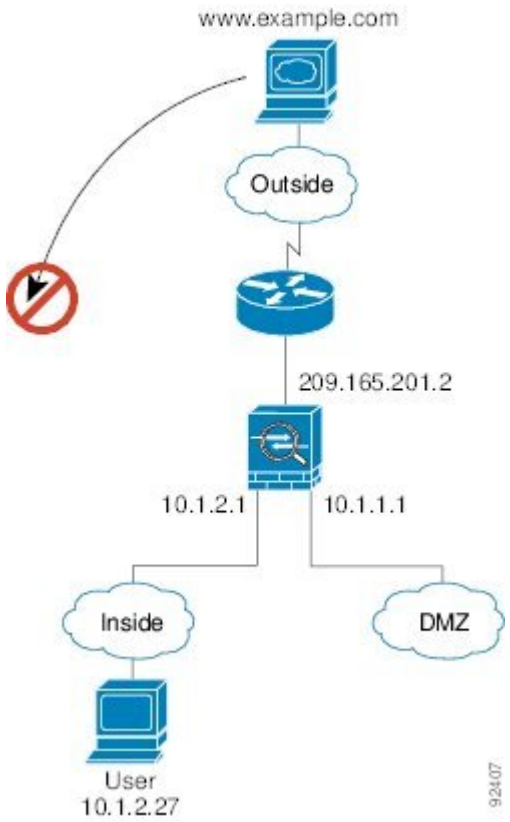
1. Un utilisateur sur le réseau interne demande une page Web au serveur web DMZ en utilisant l'adresse de destination 10.1.1.3.
2. L'ASA reçoit le paquet et, comme il s'agit d'une nouvelle session, l'ASA vérifie que le paquet est autorisé selon les conditions de la politique de sécurité.

   Pour le mode de contexte multiple, l'ASA classe d'abord le paquet dans un contexte.
3. L'ASA enregistre ensuite qu'une session est établie et transfère le paquet de l'interface DMZ.
4. Lorsque le serveur web DMZ répond à la demande, le paquet emprunte le chemin d'accès rapide, ce qui lui permet de contourner les nombreuses recherches associées à une nouvelle connexion.
5. L'ASA transmet le paquet à l'utilisateur interne.

Un utilisateur externe tente d'accéder à un hôte interne

La figure suivante montre un utilisateur externe qui tente d'accéder au réseau interne.

Illustration 8 : De l'extérieur vers l'intérieur



Les étapes suivantes décrivent comment les données passent par l'ASA :

1. Un utilisateur sur le réseau externe tente d'atteindre un hôte interne (en supposant que l'hôte a une adresse IP routable).

   Si le réseau interne utilise des adresses privées, aucun utilisateur externe ne peut atteindre le réseau interne sans la NAT. L'utilisateur externe peut tenter de joindre un utilisateur interne en utilisant une session NAT existante.

2. L'ASA reçoit le paquet et, parce qu'il s'agit d'une nouvelle session, il vérifie si le paquet est autorisé conformément à la politique de sécurité.

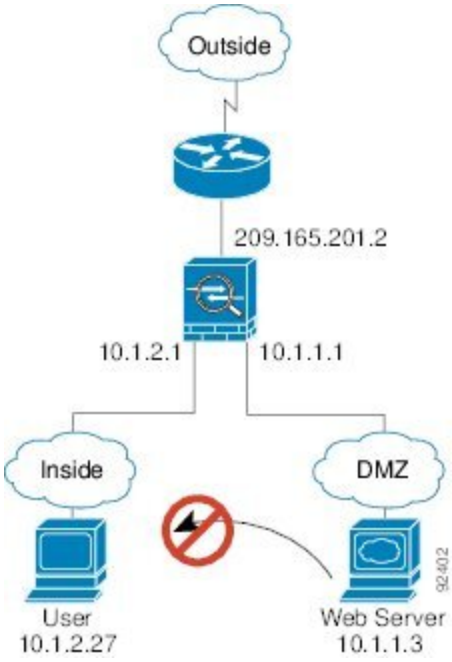
3. Le paquet est refusé et l'ASA abandonne le paquet et consigne la tentative de connexion.

   Si l'utilisateur externe tente d'attaquer le réseau interne, l'ASA utilise de nombreuses technologies pour déterminer si un paquet est valide pour une session déjà établie.

Un utilisateur DMZ tente d'accéder à un hôte interne

La figure suivante montre un utilisateur dans la DMZ tente d'accéder au réseau interne.

Illustration 9 : DMZ vers interne



Les étapes suivantes décrivent comment les données passent par l'ASA :

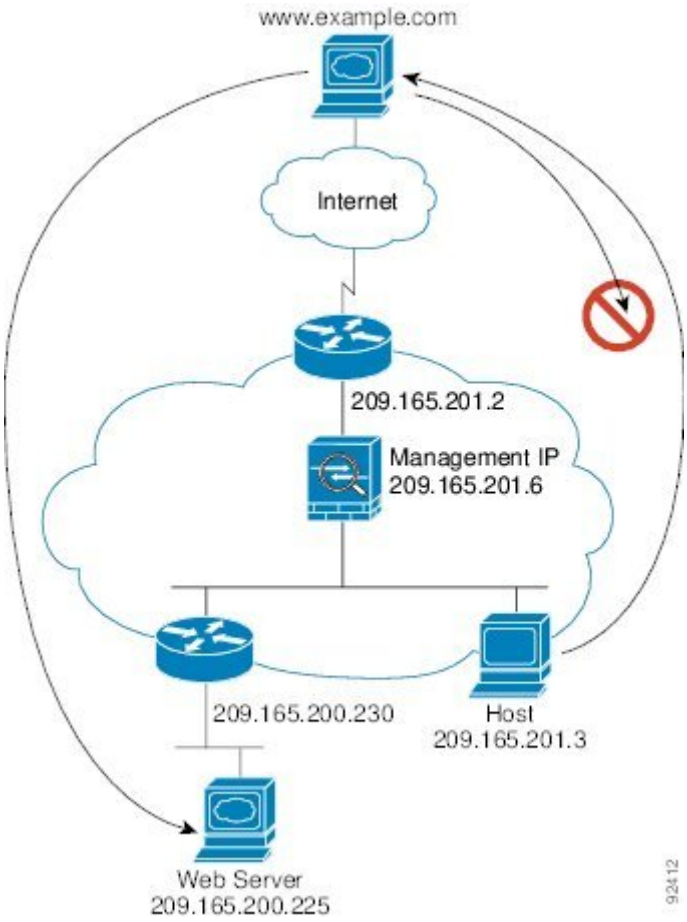
1. Un utilisateur sur le réseau DMZ tente d'atteindre un hôte interne. Étant donné que la DMZ n'a pas à acheminer le trafic sur Internet, le système d'adressage privé n'empêche pas le routage.
2. L'ASA reçoit le paquet et, parce qu'il s'agit d'une nouvelle session, il vérifie si le paquet est autorisé conformément à la politique de sécurité.

   Le paquet est refusé et l'ASA abandonne le paquet et consigne la tentative de connexion.

Progression des données dans le pare-feu transparent

La figure suivante montre une implémentation type de pare-feu transparent avec un réseau interne contenant un serveur Web public. L'ASA comporte un critère d'accès afin que les utilisateurs internes puissent accéder aux ressources Internet. Un autre critère d'accès permet aux utilisateurs externes d'accéder uniquement au serveur Web sur le réseau interne.

Illustration 10 : Chemin de données type d'un pare-feu transparent

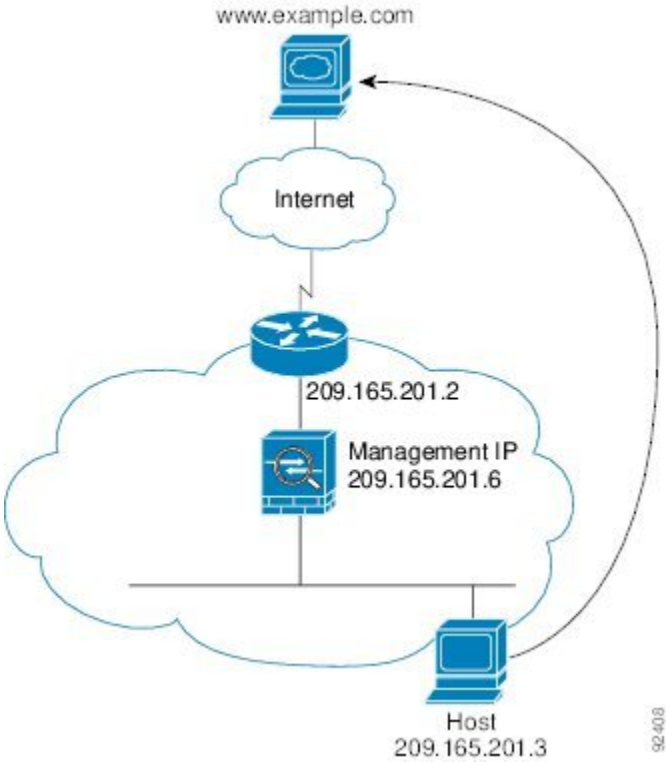


Les sections suivantes décrivent comment les données passent par l'ASA.

Un utilisateur interne visite un serveur web

La figure suivante montre un utilisateur interne accédant à un serveur web externe.

Illustration 11 : De l'intérieur vers l'extérieur



Les étapes suivantes décrivent comment les données passent par l'ASA :

1. L'utilisateur sur le réseau interne demande une page Web à www.exemple.com.
2. L'ASA reçoit le paquet et ajoute l'adresse MAC source au tableau d'adresses MAC, le cas échéant. Comme il s'agit d'une nouvelle session, il vérifie que le paquet est autorisé selon les conditions de la politique de sécurité.

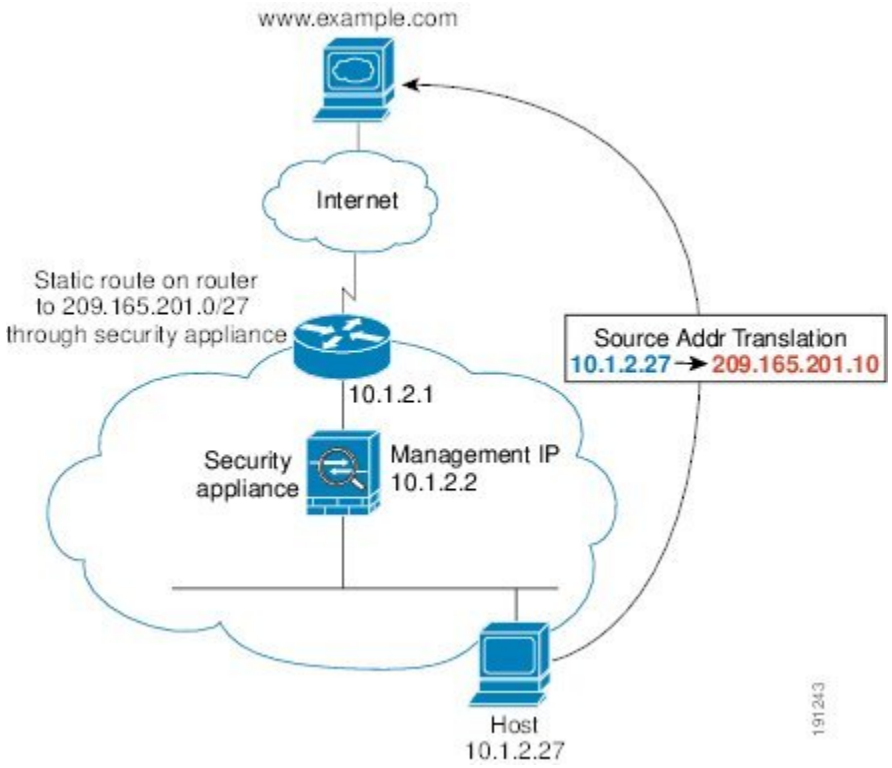
   Pour le mode de contexte multiple, l'ASA classe d'abord le paquet dans un contexte.
3. L'ASA enregistre qu'une session est établie.
4. Si l'adresse MAC de destination se trouve dans son tableau, l'ASA transfère le paquet hors de l'interface externe. L'adresse MAC de destination est celle du routeur en amont, 209.165.201.2.

   Si l'adresse MAC de destination ne se trouve pas dans le tableau ASA, il tente de découvrir l'adresse MAC en envoyant une requête ARP ou un message Ping. Le premier paquet est abandonné.
5. Le serveur web répond à la demande; comme la session est déjà établie, le paquet contourne les nombreuses recherches associées à une nouvelle connexion.
6. L'ASA transmet le paquet à l'utilisateur interne.

Un utilisateur interne visite un serveur web à l'aide de la NAT

La figure suivante montre un utilisateur interne accédant à un serveur web externe.

Illustration 12 : De l'intérieur à l'extérieur avec la NAT



Les étapes suivantes décrivent comment les données passent par l'ASA :

1. L'utilisateur sur le réseau interne demande une page Web à www.exemple.com.
2. L'ASA reçoit le paquet et ajoute l'adresse MAC source au tableau d'adresses MAC, le cas échéant. Comme il s'agit d'une nouvelle session, il vérifie que le paquet est autorisé selon les conditions de la politique de sécurité.

   Pour le mode de contexte multiple, l'ASA classe d'abord le paquet selon une interface unique.
3. L'ASA traduit l'adresse réelle (10.1.2.27) en adresse mappée 209.165.201.10.

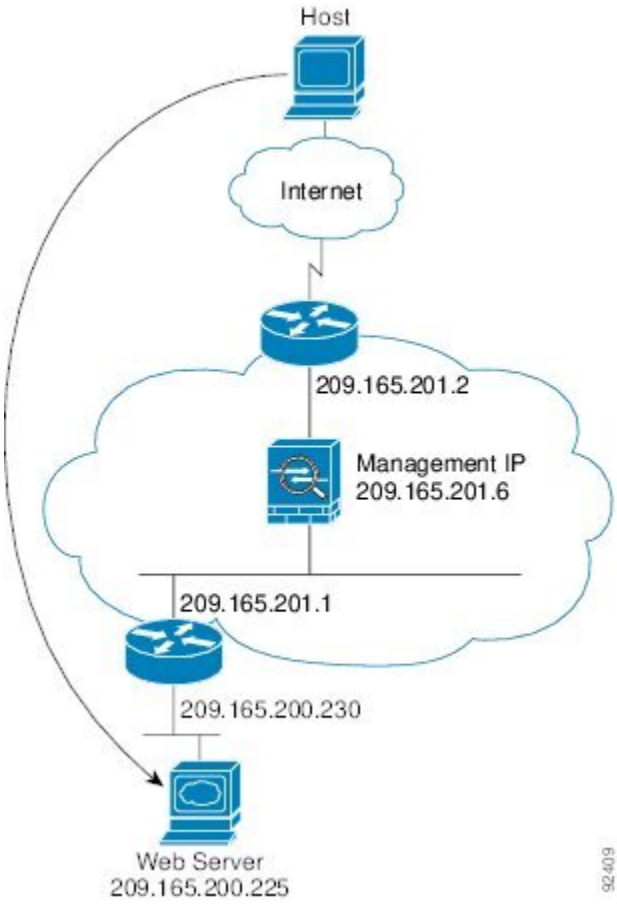
   Étant donné que l'adresse mappée ne se trouve pas sur le même réseau que l'interface externe, assurez-vous que le routeur en amont a une route statique vers le réseau mappé qui pointe vers l'ASA.
4. L'ASA enregistre ensuite qu'une session est établie et transfère le paquet de l'interface externe.
5. Si l'adresse MAC de destination se trouve dans son tableau, l'ASA transfère le paquet hors de l'interface externe. L'adresse MAC de destination est celle du routeur en amont, 10.1.2.1.

   Si l'adresse MAC de destination ne se trouve pas dans le tableau ASA, il tente alors de découvrir l'adresse MAC en envoyant une requête ARP et un message Ping. Le premier paquet est abandonné.
6. Le serveur web répond à la demande; comme la session est déjà établie, le paquet contourne les nombreuses recherches associées à une nouvelle connexion.
7. L'ASA effectue la NAT en ne traduisant pas l'adresse mappée en adresse réelle, 10.1.2.27.

Un utilisateur externe visite un serveur web sur le réseau interne

La figure suivante montre un utilisateur externe accédant au serveur web interne.

Illustration 13 : De l'extérieur vers l'intérieur



Les étapes suivantes décrivent comment les données passent par l'ASA :

1. Un utilisateur sur le réseau externe demande une page Web au serveur web interne.
2. L'ASA reçoit le paquet et ajoute l'adresse MAC source au tableau d'adresses MAC, le cas échéant. Comme il s'agit d'une nouvelle session, il vérifie que le paquet est autorisé selon les conditions de la politique de sécurité.

   Pour le mode de contexte multiple, l'ASA classe d'abord le paquet dans un contexte.
3. L'ASA enregistre qu'une session est établie.
4. Si l'adresse MAC de destination se trouve dans son tableau, l'ASA transfère le paquet hors de l'interface interne. L'adresse MAC de destination est celle du routeur en aval, 209.165.201.1.

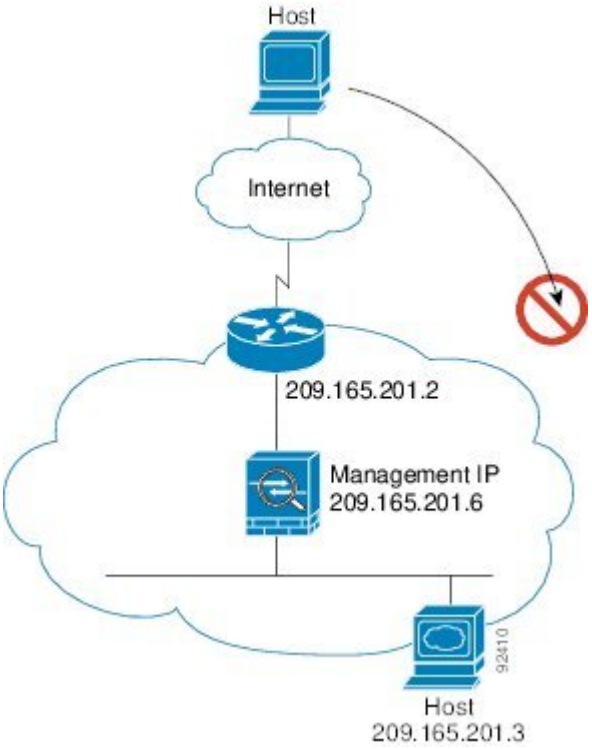
   Si l'adresse MAC de destination ne se trouve pas dans le tableau ASA, il tente alors de découvrir l'adresse MAC en envoyant une requête ARP et un message Ping. Le premier paquet est abandonné.
5. Le serveur web répond à la demande; comme la session est déjà établie, le paquet contourne les nombreuses recherches associées à une nouvelle connexion.

6. L'ASA transmet le paquet à l'utilisateur externe.

Un utilisateur externe tente d'accéder à un hôte interne

La figure suivante montre un utilisateur externe qui tente d'accéder à un hôte sur le réseau interne.

Illustration 14 : De l'extérieur vers l'intérieur



Les étapes suivantes décrivent comment les données passent par l'ASA :

1. Un utilisateur sur le réseau externe tente d'atteindre un hôte interne.
2. L'ASA reçoit le paquet et ajoute l'adresse MAC source au tableau d'adresses MAC, le cas échéant. Comme il s'agit d'une nouvelle session, il vérifie que le paquet est autorisé selon les conditions de la politique de sécurité.

   Pour le mode de contexte multiple, l'ASA classe d'abord le paquet dans un contexte.
3. Le paquet est refusé, car aucun critère d'accès n'autorise l'hôte externe, et l'ASA abandonne le paquet.
4. Si l'utilisateur externe tente d'attaquer le réseau interne, l'ASA utilise de nombreuses technologies pour déterminer si un paquet est valide pour une session déjà établie.

Historique du mode de pare-feu

Tableau 3 : Historique des fonctionnalités du mode de pare-feu

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Mode de pare-feu transparent	7.0(1)	Un pare-feu transparent est un pare-feu de couche 2 qui agit comme une « présence sur le réseau câblé » ou un « pare-feu furtif », et qui n'est pas considéré comme un saut de routeur vers les appareils connectés. Nous avons introduit les commandes suivantes : **firewall transparent**, **show firewall**. Vous ne pouvez pas définir le mode de pare-feu dans ASDM; vous devez utiliser l'interface de ligne de commande.
Groupes de ponts de pare-feu transparents	v 8.4(1)	Si vous ne souhaitez pas le surdébit des contextes de sécurité ou si vous souhaitez optimiser votre utilisation des contextes de sécurité, vous pouvez regrouper les interfaces dans un groupe de ponts, puis configurer plusieurs groupes de ponts, un pour chaque réseau. Le trafic de groupe de ponts est isolé des autres groupes de ponts. Vous pouvez configurer jusqu'à 8 groupes de ponts en mode unique ou par contexte en mode multiple, avec 4 interfaces au maximum par groupe de ponts. **Remarque** Bien que vous puissiez configurer plusieurs groupes de ponts sur l'ASA 5505, la restriction de 2 interfaces de données en mode transparent sur l'ASA 5505 signifie que vous ne pouvez utiliser efficacement qu'un seul groupe de ponts. Nous avons modifié ou introduit les écrans suivants : Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces Configuration (Configuration des interfaces) > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces > Add/Edit Bridge Group Interface (Ajouter/modifier l'interface de groupe de ponts) Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces > Add/Edit Interface (Ajouter/modifier l'interface)

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Prise en charge du mode de pare-feu mixte en mode de contexte multiple	8.5(1)/9.0(1)	Vous pouvez définir le mode de pare-feu indépendamment pour chaque contexte de sécurité en mode de contexte multiple, de sorte que certains puissent s'exécuter en mode transparent et que d'autres s'exécutent en mode routé. Nous avons modifié la commande suivante : **firewall transparent**. Pour le mode unique, vous ne pouvez pas définir le mode de pare-feu dans ASDM; vous devez utiliser l'interface de ligne de commande. Pour le mode multiple, nous avons modifié l'écran suivant : Configuration > Context Management (Gestion des contextes) > Security Contexts (Contextes de sécurité).
Nombre maximum de groupes de ponts en mode transparent augmenté à 250	9.3(1)	Le nombre maximum de groupes de ponts est passé de 8 à 250 groupes de ponts. Vous pouvez configurer jusqu'à 250 groupes de ponts en mode unique ou par contexte en mode multiple, avec 4 interfaces maximum par groupe de ponts. Nous avons modifié les écrans suivants : Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces Configuration (Configuration des interfaces) > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces > Add/Edit Bridge Group Interface (Ajouter/modifier l'interface de groupe de ponts) Configuration > Device Setup (Configuration de l'appareil) > Interface Settings (Paramètres d'interface) > Interfaces > Add/Edit Interface (Ajouter/modifier l'interface)
Nombre maximum d'interfaces en mode transparent par groupe de ponts augmenté à 64	9.6(2)	Le nombre maximum d'interfaces par groupe de ponts est passé de 4 à 64. Nous n'avons pas modifié d'écrans.

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Routage et pont intégrés	9.7(1)	Le routage et le pont intégrés permettent d'effectuer le routage entre un groupe de ponts et une interface routée. Un groupe de ponts est un groupe d'interfaces que l'ASA relie par des ponts au lieu de routes. L'ASA n'est pas un vrai pont, car l'ASA continue d'agir comme un pare-feu : le contrôle d'accès entre les interfaces est contrôlé et toutes les vérifications de pare-feu usuelles sont en place. Auparavant, vous ne pouviez configurer les groupes de ponts qu'en mode de pare-feu transparent, où vous ne pouvez pas effectuer d'acheminement entre les groupes de ponts. Cette fonctionnalité vous permet de configurer des groupes de ponts en mode de pare-feu routé et pour effectuer le routage entre des groupes de ponts et entre un groupe de ponts et une interface routée. Le groupe de ponts participe au routage en utilisant une interface virtuelle de pont (BVI) pour servir de passerelle au groupe de ponts. Le routage et le pont intégrés offrent une solution de rechange au commutateur de couche 2 externe si vous avez des interfaces supplémentaires sur l'ASA à affecter au groupe de ponts. En mode routé, les BVI peuvent être une interface nommée et participer séparément des interfaces membres à certaines fonctionnalités, telles que les règles d'accès et le serveur DHCP. Les fonctionnalités suivantes, prises en charge en mode transparent, ne sont pas prises en charge en mode routé : mode de contexte multiple, mise en grappe d'ASA. Les fonctionnalités suivantes ne sont pas prises en charge sur les BVI : le routage dynamique et le routage de multidiffusion. Nous avons modifié les écrans suivants : **Configuration** > **Device Setup (Configuration de l'appareil)** > **Interface Settings (Paramètres d'interface)** > **Interfaces** **Configuration** > **Device Setup (Configuration de l'appareil)** > **Routing (Routage)** > **Static Routes (Routes statiques)** **Configuration** > **Device Management (Gestion des périphériques)** > **DHCP** > **DHCP Server (Serveur DHCP)** **Configuration** > **Firewall (Pare-feu)** > **Access Rules (Critères d'accès)** **Configuration** > **Firewall (Pare-feu)** > **EtherType Rules (Règles EtherType)**

Nom de la caractéristique	Versions de plateforme	Renseignements sur les fonctionnalités
Prise en charge du déploiement en mode transparent pour un dispositif logique Firepower 4100/9300 ASA	9.10(1)	Vous pouvez désormais spécifier le mode transparent ou routé lorsque vous déployez l'ASA sur un Firepower 4100/9300 Écrans nouveaux ou modifiés de Firepower Chassis Manager : **Logical Devices (Dispositifs logiques)** > **Add Device (Ajouter un périphérique)** > **Settings (Paramètres)** Options nouvelles ou modifiées : liste déroulante **Firewall Mode**

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.