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.

Remarque Le mode de pare-feu affecte uniquement les interfaces de pare-feu standard, et non les interfaces IPS uniquement, comme les ensembles en ligne ou les interfaces passives. Les interfaces IPS uniquement peuvent être utilisées dans les deux modes de pare-feu. Reportez-vous à Ensembles en ligne et interfaces passives pour obtenir plus de renseignements sur les interfaces IPS-uniquement. Les ensembles en ligne vous sont peut-être familiers sous le nom d'« ensembles en ligne transparents », mais le type d'interface en ligne n'est pas lié au mode de pare-feu transparent décrit dans ce chapitre ni aux interfaces de type pare-feu.

Attention

- Utilisez les commandes CLI FTD pour définir le « mode de pare-feu ».

- À propos du mode pare-feu, à la page 1
- Paramètres d'usine, à la page 9
- Lignes directrices sur le mode pare-feu, à la page 9
- Définir le mode pare-feu, à la page 10

À propos du mode pare-feu

Le défense contre les menaces prend en charge deux modes de pare-feu pour les interfaces de pare-feu standard : le mode de pare-feu routé et le mode de pare-feu transparent.

À propos du mode de pare-feu routé

En mode routage, l'appareil de défense contre les menaces 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.

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'appareil de défense contre les menaces 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 appareil de défense contre les menaces

entre les BVI et les interfaces de routage normales. Si vous n'avez pas besoin du ou de mise en grappe, ni d'interfaces membre EtherChannel , 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.

À propos du 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.

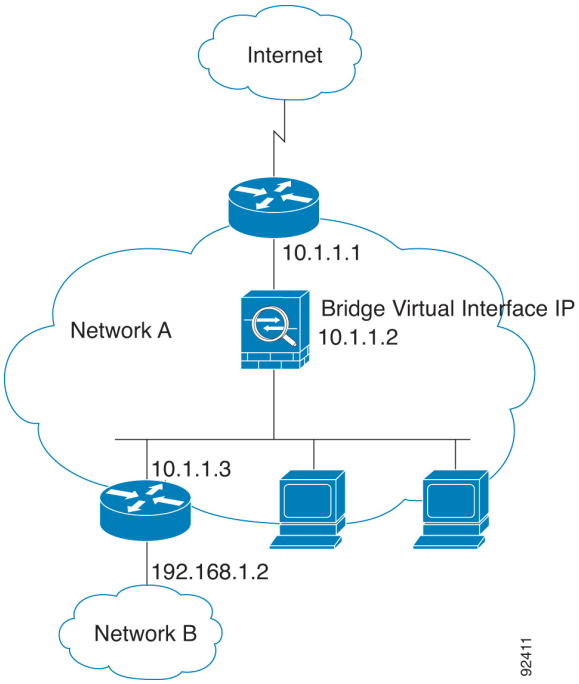
La connectivité de couche 2 est obtenue à l'aide d'un « groupe de ponts » où vous regroupez les interfaces interne et externe d'un réseau, où l'appareil de défense contre les menaces utilise des techniques de pont pour acheminer le trafic entre les interfaces. Chaque groupe de ponts comprend une interface 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 du pare-feu transparent au sein de votre réseau

L'appareil de défense contre les menaces 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



Trafic de transfert 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. 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 le appareil de défense contre les menaces .

À propos des groupes de ponts

Un groupe de ponts est un groupe d'interfaces que appareil de défense contre les menaces 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.

Interface BVI (Bridge Virtual Interface)

Chaque groupe de ponts comprend une interface virtuelle de pont (BVI). appareil de défense contre les menaces 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.

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 :

- 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 appareil de défense contre les menaces : lorsque vous spécifiez un serveur syslog (ou un serveur SNMP, ou un autre service où le trafic provient de appareil de défense contre les menaces), vous pouvez spécifier une interface BVI ou une interface membre.

Si vous ne nommez pas les BVI en mode routé, appareil de défense contre les menaces 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 ni de mise en grappe, ni d'interfaces membre EtherChannel, 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

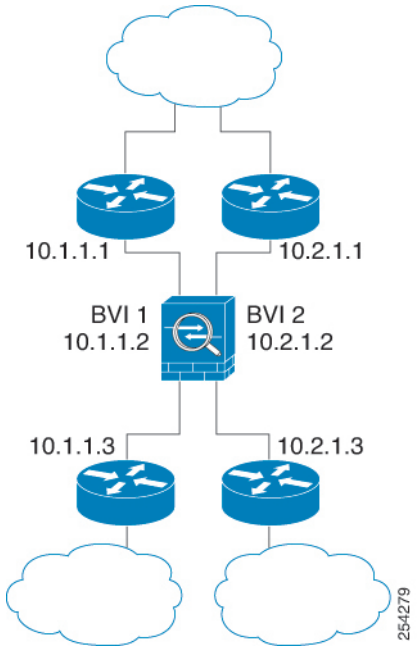
Le trafic des groupes de ponts est isolé des autres groupes de ponts; le trafic n'est pas acheminé vers un autre groupe de ponts dans appareil de défense contre les menaces , et le trafic doit quitter appareil de défense contre les menaces avant d'être acheminé par un routeur externe vers un autre groupe de ponts dans appareil de

défense contre les menaces . 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.

Vous pouvez inclure plusieurs interfaces par groupe de ponts. Consultez Lignes directrices sur le mode pare-feu, à la page 9 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 appareil de défense contre les menaces , qui comporte deux groupes de ponts.

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

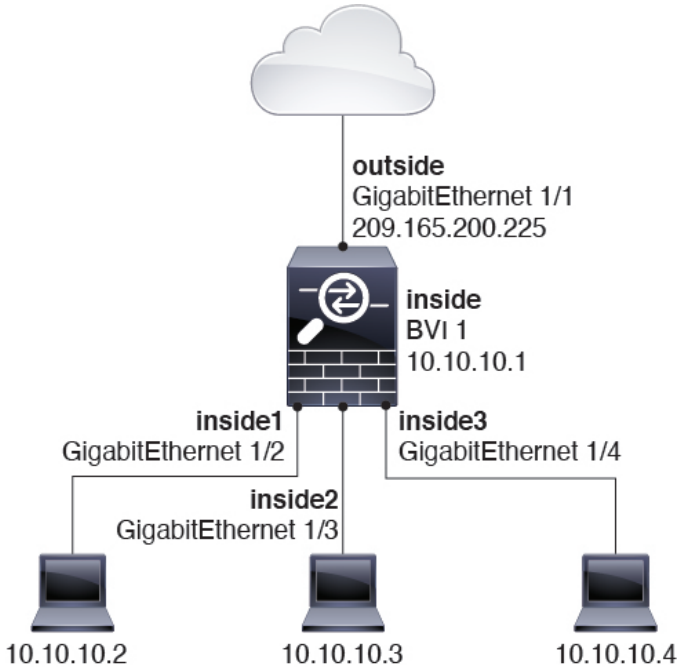


Groupes de ponts en mode pare-feu routé

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.

Une des utilisations d'un groupe de ponts en mode routé est d'utiliser des interfaces supplémentaires sur défense contre les menaces 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.

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



Autorisation du trafic de couche 3

- Le trafic en monodiffusion IPv4 et IPv6 nécessite une règle d'accès pour être autorisé à traverser le groupe de ponts.
- 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 5). 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

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.

Par défaut, les BPDU sont aussi acheminées pour l'inspection avancée, ce qui est inutile pour ce type de paquets, et peut entraîner des problèmes si elles sont bloquées en raison d'un redémarrage de l'inspection, par exemple. Nous vous recommandons de toujours exempter les BPDU de l'inspection avancée. Pour ce faire, utilisez FlexConfig pour configurer une liste de contrôle d'accès EtherType qui fait confiance aux BPDU et les exempte de l'inspection avancée sur chaque interface membre. Consultez #unique_433.

L'objet FlexConfig doit déployer les commandes suivantes, où vous devez remplacer <if-name> par un nom d'interface. Ajoutez autant de commandes access-group que nécessaire pour couvrir chaque interface de membre de groupe de ponts sur le périphérique. Vous pouvez également choisir un nom différent pour la liste de contrôle d'accès.

```
access-list permit-bpdu ethertype trust bpdu
access-group permit-bpdu in interface <if-name>
```

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'appareil de défense contre les menaces : ajoutez une voie de routage statique/par défaut sur l'appareil de défense contre les menaces pour le trafic destiné à un réseau distant où se trouve un serveur syslog, par exemple.
- Trafic de voix sur IP (VoIP) et TFTP, et le point terminal se trouve à au moins un saut (ajouter une route statique sur l'appareil de défense contre les menaces pour le trafic destiné au point terminal distant afin que les connexions secondaires soient réussies. L'appareil de défense contre les menaces 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'appareil de défense contre les menaces doit effectuer une recherche de routage pour installer le sténopé sur la bonne interface.

  Parmi les autres applications concernées, on trouve :

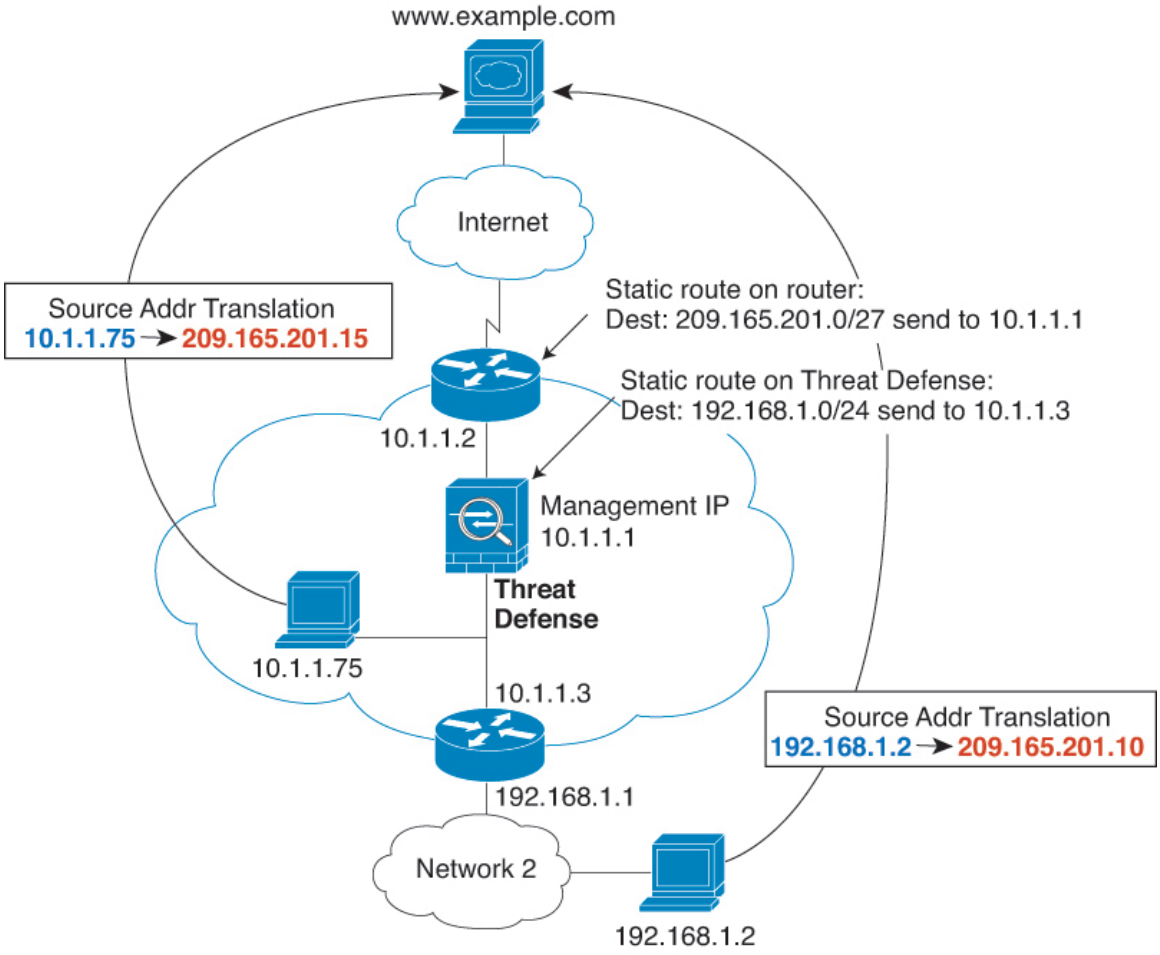
  - H.323
  - RTSP
  - SIP
  - Skinny (SCCP)
  - SQL*Net
  - SunRPC
  - TFTP

- Trafic à au moins un saut de distance pour lequel l'appareil de défense contre les menaces exécute la NAT - Configurer une route statique sur l'appareil de défense contre les menaces 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'appareil de défense contre les menaces .

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

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	—

Fonctionnalités	Description
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 appareil de défense contre les menaces pour les membres des groupes de ponts. Vous pouvez également autoriser les protocoles de routage dynamique à l'aide de appareil de défense contre les menaces en utilisant une règle d'accès.
Routage de multidiffusion IP	Vous pouvez autoriser le trafic en multidiffusion via l'appareil de défense contre les menaces 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 appareil de défense contre les menaces . Vous pouvez faire passer le trafic VPN par l'ASA à l'aide d'une règle d'accès, mais cela ne met pas fin aux connexions hors gestion.

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

Le tableau suivant répertorie les fonctions 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	Seules les interfaces physiques, les interfaces redondantes et les sous-interfaces sont prises en charge en tant qu'interfaces de membres de groupes de ponts. Les interfaces Diagnostic ne sont pas non plus prises en charge.
Mise en grappes	Les groupes de ponts ne sont pas pris en charge dans la mise en grappe.
DNS dynamique	—
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 appareil de défense contre les menaces en utilisant une règle d'accès. Les interfaces de groupe sans pont prennent en charge le routage dynamique.

Fonctionnalités	Description
Routage de multidiffusion IP	Vous pouvez autoriser le trafic en multidiffusion via l'appareil de défense contre les menaces en l'autorisant dans une règle d'accès. Les interfaces de groupe sans pont prennent en charge le routage de multidiffusion.
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 appareil de défense contre les menaces . 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.

Paramètres d'usine

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

Directives de groupe de ponts (modes transparent et routé)

- Vous pouvez créer jusqu'à 250 groupes de ponts, avec interfaces par groupe de ponts.
- Chaque réseau connecté directement doit se trouver sur le même sous-réseau.
- L'appareil de défense contre les menaces 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.
- Une adresse IP pour les 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 appareil de défense contre les menaces . 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).
- Les interfaces de gestion ne sont pas prises en charge en tant que membres de groupes de ponts.
- En mode multi-instance, les interfaces partagées ne sont pas prises en charge pour les interfaces des membres des groupes de ponts (en mode transparent ou en mode routé).

- Pour défense contre les menaces virtuelles sur VMware avec 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.
- Dans le cas du Firepower 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.
- Pour Firepower 4100/9300, les interfaces de partage de données ne sont pas prises en charge en tant que membres de groupes de ponts.
- 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 défense contre les menaces 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 Diagnostic.
- Le mode transparent n’est pas pris en charge sur les instances virtuelles de défense contre les menaces déployées sur Amazon Web Services, Microsoft Azure, Google Cloud Platform et Oracle Cloud Infrastructure.
- 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 défense contre les menaces 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.
- Les paquets écho de la détection de transfert bidirectionnel (BFD) ne sont pas autorisés par le biais de défense contre les menaces lors de l’utilisation de membres de groupe de ponts. S’il y a deux voisins de chaque côté de défense contre les menaces exécutant BFD, alors défense contre les menaces 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 pare-feu

Vous pouvez définir le mode de pare-feu lorsque vous effectuez la configuration initiale du système au niveau de l’interface de ligne de commande. Nous vous recommandons de définir le mode de pare-feu lors de l’installation, car la modification du mode de pare-feu efface votre configuration et vous évite d’avoir des paramètres incompatibles. Si vous devez modifier le mode de pare-feu ultérieurement, vous devez le faire à partir de la CLI.

Procédure

Étape 1 Désinscrire le périphérique défense contre les menaces de centre de gestion.

Vous ne pouvez pas changer de mode avant d'avoir annulé l'enregistrement du périphérique.

a) Choisissez **Devices (périphériques)** > **Device Management (gestion des périphériques)**.

b) À côté du périphérique que vous souhaitez désinscrire, cliquez sur **Plus** (⋮), puis sur **Delete** (Supprimer).

Étape 2 Accédez à l'interface de ligne de commande défense contre les menaces du périphérique, de préférence à partir du port de console.

Si vous utilisez SSH pour l'interface de dépistage, la modification de mode efface la configuration de votre interface et vous serez déconnecté. Vous devez plutôt vous connecter à l'interface de gestion.

Étape 3 Modifiez le mode de pare-feu :

configure firewall [**routed** | **transparent**]

Exemple :

```
> configure firewall transparent
This will destroy the current interface configurations, are you sure that you want to
proceed? [y/N] y
The firewall mode was changed successfully.
```

Étape 4 Réinscrivez-vous à l'aide de centre de gestion.

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.