Client ou serveur DHCP avec configuration de routeur ZBF

Table des matières

Introduction

Ce document décrit comment configurer un routeur qui agit en tant que serveur DHCP (Dynamic Host Control Protocol) ou client DHCP avec la fonctionnalité de pare-feu de zone (ZBF). Étant donné qu'il est assez courant d'avoir DHCP et ZBF activés simultanément, ces conseils de configuration aident à garantir que ces fonctionnalités interagissent correctement.

Conditions préalables

Exigences

Cisco vous recommande de connaître le pare-feu de zone du logiciel Cisco IOS®. Reportez-vous au Guide de conception et d'application du pare-feu de stratégie basée sur les zones pour plus de détails.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informations sur les fonctionnalités

Lorsque ZBF est activé sur un routeur IOS, tout trafic vers la zone self (c'est-à-dire le trafic destiné au plan de gestion du routeur) est autorisé par défaut dans le train de codes IOS 15.x.

Si vous avez créé une stratégie pour une zone (telle que « interne » ou « externe ») vers la zone auto (stratégie « out-to-self ») ou l'inverse (stratégie « self-to-out »), vous devez définir explicitement le trafic autorisé dans les stratégies associées à ces zones. Utilisez l'action Contrôler ou Autoriser afin de définir le trafic autorisé.

Analyse des données

Le protocole DHCP utilise des paquets UDP (User Datagram Protocol) de diffusion afin de terminer le processus DHCP. Les configurations de pare-feu basées sur les zones qui spécifient l'action d'inspection pour ces paquets UDP de diffusion peuvent être abandonnées par le routeur et le processus DHCP peut échouer. Ce message de journal peut également s'afficher :

```
%FW-6-DROP_PKT: Dropping udp session 0.0.0.0:68 255.255.255.255:67 on zone-pair
self-out class dhcp with ip ident 0
```

Reportez-vous au problème décrit dans le bogue Cisco ayant l'ID CSCso53376, « ZBF inspect does not work for broadcast traffic ».

Afin d'éviter ce problème, modifiez la configuration du pare-feu basé sur les zones de sorte que l'action de passage au lieu de l'action d'inspection soit appliquée au trafic DHCP.

> **Remarque** : cette opération n'est nécessaire que lorsqu'une stratégie est appliquée à la zone self du routeur.

Pare-feu basé sur les zones en tant que client DHCP avec action de passe pour le trafic UDP

Configurer

Cet exemple de configuration utilise l'action pass au lieu de l'action inspect dans le policy-map pour tout le trafic UDP en provenance ou à destination du routeur.

```
zone security outside
```

```
zone security inside

interface Ethernet0/1
zone-member security outside
interface Ethernet0/2
zone-member security inside

class-map type inspect match-all dhcp
match protocol udp

policy-map type inspect out-to-self
class type inspect dhcp
pass
class class-default
drop
policy-map type inspect self-to-out
class type inspect dhcp
pass
class class-default
drop

zone-pair security out-to-self source outside destination self
service-policy type inspect out-to-self
zone-pair security self-to-out source self destination outside
service-policy type inspect self-to-out
```

Vérifier

Passez en revue les syslogs afin de vérifier que le routeur a obtenu une adresse DHCP.

Lorsque les politiques « out-to-self » et « self-to-out » sont toutes deux configurées pour transmettre le trafic UDP, le routeur peut obtenir une adresse IP auprès de DHCP, comme indiqué dans le journal système suivant :

```
%DHCP-6-ADDRESS_ASSIGN: Interface Ethernet1/0 assigned DHCP address 192.168.1.5,
mask 255.255.255.0
```

Lorsque seule la stratégie de zone out-to-self est configurée pour transmettre le trafic UDP, le routeur peut également obtenir une adresse IP auprès de DHCP et ce syslog est créé :

```
%DHCP-6-ADDRESS_ASSIGN: Interface Ethernet1/0 assigned DHCP address 192.168.1.6,
mask 255.255.255.0
```

Lorsque seule la politique de zone auto-vers-sortie est configurée pour transmettre le trafic UDP, le routeur peut obtenir une adresse IP auprès de DHCP et ce syslog est créé :

```
%DHCP-6-ADDRESS_ASSIGN: Interface Ethernet1/0 assigned DHCP address 192.168.1.7,
mask 255.255.25
```

Pare-feu basé sur les zones avec action Pass pour le trafic DHCP

Configurer

Cet exemple de configuration montre comment empêcher tout trafic UDP d'une zone vers la zone propre à votre routeur, à l'exception des paquets DHCP. Utilisez une liste d'accès avec des ports spécifiques afin d'autoriser uniquement le trafic DHCP ; dans cet exemple, les ports UDP 67 et UDP 68 sont spécifiés pour être mis en correspondance. L'action de passage est appliquée à un class-map qui référence la liste de contrôle d'accès.

```
access-list extended 111
 10 permit udp any any eq 67

access-list extended 112
 10 permit udp any any eq 68

class-map type inspect match-any self-to-out
match access-group 111
class-map type inspect match-any out-to-self
match access-group 112

zone security outside
zone security inside

interface Ethernet0/1
zone-member security outside
interface Ethernet0/2
zone-member security inside

policy-map type inspect out-to-self
class type inspect out-to-self
pass
class class-default
drop
policy-map type inspect self-to-out
class type inspect self-to-out
pass
class class-default
drop

zone-pair security out-to-self source outside destination self
service-policy type inspect out-to-self
zone-pair security self-to-out source self destination outside
service-policy type inspect self-to-out
```

Vérifier

Examinez le résultat de la commande **show policy-map type inspect zone-pair sessions** afin de confirmer que le routeur autorise le trafic DHCP à travers le pare-feu de zone. Dans cet exemple de sortie, les compteurs mis en surbrillance indiquent que les paquets sont passés à travers le pare-feu de zone. Si ces compteurs sont à zéro, la configuration présente un problème ou les paquets n’arrivent pas au routeur pour y être traités.

```
router#show policy-map type inspect zone-pair sessions

policy exists on zp out-to-self
Zone-pair: out-to-self
Service-policy inspect : out-to-self
Class-map: out-to-self (match-any)
Match: access-group 112
3 packets, 924 bytes
30 second rate 0 bps
```

```
Pass
6 packets, 1848 bytes

Class-map: class-default (match-any)
Match: any
Drop
0 packets, 0 bytes

policy exists on zp self-to-out
Zone-pair: self-to-out
Service-policy inspect : self-to-out
Class-map: self-to-out (match-any)
Match: access-group 111
6 packets, 3504 bytes
30 second rate 0 bps
Pass
6 packets, 3504 bytes

Class-map: class-default (match-any)
Match: any
Drop
0 packets, 0 bytes
```

Scénario de configurations incorrectes

Cet exemple de scénario montre ce qui se passe lorsque le routeur est mal configuré pour spécifier l'action d'inspection du trafic DHCP. Dans ce scénario, le routeur est configuré comme client DHCP. Le routeur envoie un message de détection DHCP pour tenter d'obtenir une adresse IP. Le pare-feu de zone est configuré pour inspecter ce trafic DHCP. Voici un exemple de configuration ZBF :

```
zone security outside
zone security inside

interface Ethernet0/1
zone-member security outside

interface Ethernet0/2
zone-member security inside

class-map type inspect match-all dhcp
match protocol udp

policy-map type inspect out-to-self
class type inspect dhcp
inspect
class class-default
drop
policy-map type inspect self-to-out
class type inspect dhcp
inspect
class class-default
drop

zone-pair securiy out-to-self source outside destination self
service-policy type inspect out-to-self
zone-pair security self-to-out source self destination outside
service-policy type inspect self-to-out
```

Lorsque la politique d'auto-détection des appels sortants est configurée avec l'action d'inspection

du trafic UDP, le paquet de détection DHCP est abandonné et ce syslog est créé :

```
%FW-6-DROP_PKT: Dropping udp session 0.0.0.0:68 255.255.255.255:67 on zone-pair
self-out class dhcp with ip ident 0
```

Lorsque les politiques self-to-out et out-to-self sont toutes deux configurées avec l'action d'inspection pour le trafic UDP, le paquet de détection DHCP est abandonné et ce syslog est créé :

```
%FW-6-DROP_PKT: Dropping udp session 0.0.0.0:68 255.255.255.255:67 on zone-pair
self-out class dhcp with ip ident 0
```

Lorsque l'action d'inspection est activée sur la stratégie « out-to-self » et que l'action « pass » est activée sur la stratégie « self-to-out » pour le trafic UDP, le paquet d'offre DHCP est abandonné après l'envoi du paquet de détection DHCP et ce syslog est créé :

```
%FW-6-DROP_PKT: Dropping udp session 192.168.1.1:67 255.255.255.255:68 on zone-pair
out-self class dhcp with ip ident 0
```

Routeur en tant que serveur DHCP

Si l'interface interne des routeurs agit en tant que serveur DHCP et si les clients qui se connectent à l'interface interne sont les clients DHCP, ce trafic DHCP est autorisé par défaut s'il n'y a pas de politique de zone interne-à-interne ou interne-à-interne.

Cependant, si l'une de ces politiques existe, vous devez configurer une action de passage pour le trafic d'intérêt (port UDP 67 ou port UDP 68) dans la politique de service de paire de zones.

Dépannage

Aucune information de dépannage spécifique n'est actuellement disponible pour ces configurations.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.