Contenu

Introduction

Ce document décrit comment configurer un routeur qui agit en tant que serveur ou DHCP Client du Dynamic Host Control Protocol (DHCP) avec la configuration basée sur zone du Pare-feu (ZBF). Puisqu'il est assez commun pour faire activer le DHCP et le ZBF simultanément, ces conseils de configuration aident à assurer ces caractéristiques interactives correctement.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance du Pare-feu basé sur zone de logiciel de Cisco IOS®. Référez-vous au guide basé sur zone de conception et d'application de Pare-feu de stratégie pour des détails.

Composants utilisés

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

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Les informations de caractéristique

Quand ZBF est activé sur un routeur IOS, on permet n'importe quel trafic à la zone d'individu (c'est-à-dire, le trafic destiné à l'avion de la Gestion du routeur) par défaut dans la série IOS 15.x de code.

Si vous avez créé une stratégie pour n'importe quelle zone (telle que le « intérieur » ou « dehors ") à la zone d'individu (stratégie de -à-individu) ou à l'inverse (auto-- à la stratégie), vous devez explicitement définir le trafic permis dans les stratégies reliées à ces zones. Utilisez l'examiner ou passez l'action afin de définir le trafic permis.

Analyse de données

Les utilisations DHCP ont annoncé des paquets de Protocole UDP (User Datagram Protocol) afin de compléter le processus DHCP. des configurations basées sur zone de Pare-feu qui spécifient l'action d'examiner pour ces paquets UDP d'émission pourraient être abandonnées par le routeur, et le processus DHCP pourraient échouer. Vous pourriez également voir ce message de log :

Référez-vous à la question décrite dans l'ID de bogue Cisco CSCso53376, « ZBF examinent ne fonctionnent pas pour le trafic d'émission. »

Afin d'éviter ce problème, modifiez la configuration basée sur zone de Pare-feu de sorte que l'action de passage au lieu de l'action d'examiner soit appliquée au trafic DHCP.

> Remarque: Ceci est exigé seulement quand une stratégie est appliquée à la zone d'individu sur le routeur.

Pare-feu basé sur zone comme DHCP Client avec l'action de passage pour le trafic UDP

Configurez

Cet exemple de configuration utilise le positionnement d'action de passage au lieu de l'action d'examiner dans le policy-map pour tout le trafic UDP à ou du routeur.

Vérifiez

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

Quand le -à-individu et auto-- aux stratégies sont configurés pour passer le trafic UDP, le routeur peut obtenir une adresse IP du DHCP suivant les indications de ce Syslog :

Quand seulement la stratégie de zone de -à-individu est configurée pour passer le trafic UDP, le

routeur peut également obtenir une adresse IP du DHCP, et ce Syslog est créé :

Quand seulement auto-- à la stratégie de zone est configuré pour passer le trafic UDP, le routeur peut obtenir une adresse IP du DHCP, et ce Syslog est créé :

Pare-feu basé sur zone avec l'action de passage pour le trafic DHCP

Configurez

Cet exemple de configuration affiche comment empêcher tout le trafic UDP d'une zone dans la zone de l'individu de votre routeur excepté des paquets DHCP. Employez une liste d'accès avec les ports spécifiques afin de permettre juste le trafic DHCP ; dans cet exemple, le port UDP 67 et le port UDP 68 sont spécifiés pour être appariés. Un class-map qui met en référence la liste d'accès a l'action de passage appliquée.

```
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
```

Vérifiez

Passez en revue la sortie de la commande de **sessions de show policy-map type inspect zone-pair** afin de confirmer que le routeur permet le trafic DHCP par le Pare-feu de zone. Dans cet

exemple de sortie, les compteurs mis en valeur indiquent que des paquets sont traversés le Pare-feu de zone. Si ces compteurs sont zéro, il y a un problème avec la configuration, ou les paquets n'arrivent pas au routeur pour le traitement.

```
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 pour des configurations incorrectes

Cet exemple de scénario affiche ce qui se produit quand le routeur est inexactement configuré pour spécifier l'action d'examiner pour le trafic DHCP. Dans ce scénario, le routeur est configuré comme DHCP Client. Le routeur envoie un DHCP découvrent le message pour essayer et obtenir une adresse IP. Le Pare-feu basé sur zone est configuré pour examiner ce trafic DHCP. C'est un exemple de la configuration ZBF :

```
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
```

Quand auto-- à la stratégie est configuré avec l'action d'examiner pour le trafic UDP, le paquet de détection DHCP est lâché, et ce Syslog est créé :

```
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
```

Quand la stratégie de chacun des deux auto-à- et de -à-individu sont configurées avec l'action d'examiner pour le trafic UDP, le paquet de détection DHCP est lâché, et ce Syslog est créé :

```
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
```

Quand la stratégie de -à-individu a l'action d'examiner activée, et auto-- à la stratégie a l'action de passage activée pour le trafic UDP, le paquet d'offre DHCP est lâché après que le paquet de détection DHCP soit envoyé, et ce Syslog est créé :

```
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
```

Routeur comme serveur DHCP

Si l'interface interne des Routeurs agit en tant que serveur DHCP et si les clients qui connectent à l'interface interne sont les clients DHCP, on permet ce trafic DHCP par défaut s'il n'y a aucun à

l'intérieur-à-individu ou auto-à-à l'intérieur de stratégie de zone.

Cependant, si l'un ou l'autre de ces stratégies existe, vous devez configurer une action de passage pour le trafic d'intérêt (port UDP 67 ou port UDP 68) dans la stratégie de service de paires de zone.

Dépannez

Il n'y a actuellement aucune information de dépannage spécifique disponible pour ces configurations.