FWSM : Dépannez les pannes du trafic devant faire du tort Xlates

Contenu

Introduction

En raison de la conception du traitement de paquets du Module de services de Pare-feu (FWSM), les xlates établis par inexactement des paquets routés peuvent entraîner des pannes du trafic pour des connexions par le Pare-feu. Afin de sélectionner une interface de sortie pour un paquet entrant, le FWSM vérifie d'abord pour voir si l'IP de destination du paquet entrant apparie n'importe quel IP/Network global existant dans une traduction NAT (xlate) pour cette interface dans sa table de xlate. Si une correspondance est trouvée, l'interface de sortie est simplement choisie basée sur l'interface locale dans l'entrée de xlate et le Pare-feu ne consulte pas la table de routage pour prendre la décision d'interface de sortie.

Le comportement par défaut du FWSM est d'établir une entrée de xlate pour le source ip de n'importe quel paquet permis qui est reçu sur une de ses interfaces. Si un paquet est conduit par le réseau inexactement (pour un certain nombre de raisons) et arrive d'arrivée sur l'interface fausse du FWSM, un xlate est établi pour refléter ceci. Quand ceci se produit, les entrées dans la table de xlate peuvent ignorer des entrées dans la table de routage et entraîner des pannes du trafic pour les destinations affectées.

Ce document décrit les symptômes et les déclencheurs pour cette question, comment la diagnostiquer, et fournit des solutions pour l'empêcher de se produire.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance de FWSMs.

Composants utilisés

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

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Symptômes

Topologie logique

Configuration appropriée

```
interface Vlan1
 nameif outside
 security-level 0
 ip address 192.168.100.50 255.255.255.0
!
interface Vlan10
 nameif inside
 security-level 100
 ip address 10.10.1.50 255.255.255.0
!
interface Vlan20
 nameif dmz
 security-level 50
 ip address 10.20.1.50 255.255.255.0
!
same-security-traffic permit intra-interface
access-list outside_in extended permit tcp any host 10.30.1.1 eq www
access-list inside_in extended permit ip any any
access-group inside_in in interface inside
access-group outside_in in interface outside
route outside 0.0.0.0 0.0.0.0 192.168.100.254
route dmz 10.30.1.0 255.255.255.0 10.20.1.254
```

Comportements observés

Les connexions du PC client chez 172.16.1.10 au web server chez 10.30.1.1 échouent.

Une capture de paquet sur l'interface **extérieure** affiche une synchronisation de TCP du PC client arrivant à l'interface du FWSM.

```
FWSM# show capture outside
3 packets seen, 3 packets captured
   1: 13:58:09.280752960 802.1Q vlan#1 P0 172.16.1.10.57389 > 10.30.1.1.80: S
```

```
      918518428:918518428(0) win 8192 <mss 1380,nop,nop,sackOK>
   2: 13:58:12.280755950 802.1Q vlan#1 P0 172.16.1.10.57389 > 10.30.1.1.80: S
      918518428:918518428(0) win 8192 <mss 1380,nop,nop,sackOK>
   3: 13:58:18.280761960 802.1Q vlan#1 P0 172.16.1.10.57389 > 10.30.1.1.80: S
      918518428:918518428(0) win 8192 <mss 1380,nop,nop,sackOK>
3 packets shown
```

Une capture de paquet sur l'interface de **dmz** n'affiche pas ce paquet laissant le Pare-feu.

```
FWSM# show capture dmz
0 packet seen, 0 packet captured
0 packet shown
```

Aucune entrée n'est établie dans la table de la connexion du FWSM et les Syslog n'affichent pas relatif à l'information aux adresses IP de client ou de serveur.

Déclencheurs

Àun niveau fondamental, cette question est provoqué par par une entrée dans la table du xlate du FWSM qui a été construite par inexactement un paquet routé. En raison de la manière que le traitement de paquets du FWSM est conçu, le Pare-feu vérifie la table de xlate avant qu'elle vérifie la table de routage pour déterminer l'interface de sortie. En conséquence, si un paquet apparie un xlate existant l'interface de sortie sera sélectionnée a basé sur cette entrée, même si l'entrée est en conflit avec ce qui est répertorié dans la table de routage. En d'autres termes, la table de xlate a la priorité au-dessus de la table de routage.

Afin de diagnostiquer cette question, vérifiez la sortie de la commande de **débogage de show xlate** :

```
FWSM# show xlate debug
Flags: D - DNS, d - dump, I - identity, i - inside, n - no random,
       o - outside, r - portmap, s - static
3 in use, 3 most used
NAT from inside:10.30.1.1 to outside:10.30.1.1 flags Ii idle 0:00:00 timeout 3:00:00 connections
0
NAT from inside:10.30.1.1 to inside:10.30.1.1 flags Ii idle 0:00:07 timeout 3:00:00 connections
0

NAT from dmz:10.30.1.1 to outside:10.30.1.1 flags Ii idle 0:00:10 timeout 3:00:00 connections 0
```

Remarque: Le mot clé de débogage dans le show xlate est crucial. Sans lui, les entrées de xlate n'incluront pas les noms d'interface que l'entrée est associée avec.

La table de xlate prouve qu'il y a 3 xlates établis pour le web server. Le premier xlate est établi entre l'**interface interne** et l'interface **extérieure**. Le deuxième xlate est établi comme xlate hairpinned ou u-tourné sur l'**interface interne**. Le troisième xlate est établi entre le **dmz** et l'interface **extérieure**. Je diminue indique que c'est un xlate d'identité et l'IP n'est pas traduit réellement.

La première interface répertoriée dans l'entrée est la « vraie » ou « locale » interface où l'IP est censé exister réellement. La deuxième interface répertoriée est interface « tracée » ou « globale » où l'IP est traduit. Ni l'un ni l'autre de ces xlates affichés ne sont corrects. C'est parce que le web server (10.30.1.1) existe réellement derrière l'interface de **dmz**. Le troisième xlate est correct pour cette conception de réseaux.

La panne de connexion se produit en raison du premier xlate répertorié dans la table. Quand le paquet de synchronisation du TCP du client arrive sur l'interface extérieure destinée à 10.30.1.1, le FWSM vérifie la table de xlate et apparie la première entrée. Cette entrée indique que le paquet

de sortie sur l'**interface interne**, qui est incorrecte, et le paquet blackholed.

Par défaut, le FWSM établira automatiquement un xlate d'identité pour n'importe quel trafic qui n'apparie pas une règle NAT explicitement configurée. Pour cette raison, même si un paquet arrive incorrectement sur une interface incorrecte, un xlate sera établi. Spécifiquement pour ce cas, les paquets originaires de 10.30.1.1 sont arrivés d'arrivée sur l'**interface interne** au lieu de l'arrivée sur l'interface de **dmz** comme est prévu.

Le premier xlate (**intérieur > dehors**) a été établi quand le web server essayé pour cingler une adresse IP inexistante (10.199.199.1). La requête d'écho est partie du web server destiné à sa passerelle par défaut (le routeur DMZ). Le routeur DMZ a expédié le paquet vers le routeur interne, par son artère statique :

```
S       10.0.0.0/8 [1/0] via 10.50.1.254
```

Puisque le réseau 10.199.199.0/24 n'existe pas réellement n'importe où, le routeur interne suit simplement son default route et envoie le paquet à l'**interface interne du** FWSM :

```
S*   0.0.0.0/0 [1/0] via 10.20.1.50
```

De même, le FWSM également n'a pas une artère pour le réseau de destination. Par conséquent, il sélectionne l'interface extérieure comme interface de sortie et établit un xlate d'identité de l'intérieur de **> extérieur** :

```
S    0.0.0.0 0.0.0.0 [1/0] via 192.168.100.254, outside
```

Le deuxième xlate (**intérieur > à l'intérieur**) a été établi quand le web server essayé pour accéder au serveur DNS tandis que l'interface de 10.40.1.254 du routeur interne était temporairement en bas d'en raison d'une instabilité de lien. Les DN demandent ont laissé le web server destiné à sa passerelle par défaut (le routeur DMZ). Le routeur DMZ a expédié le paquet vers le routeur interne, par son artère statique :

```
S       10.0.0.0/8 [1/0] via 10.50.1.254
```

Cependant, l'interface connectée du routeur interne au réseau 10.40.1.0/24 était temporairement vers le bas et sa directement route connectée pour ce réseau manquait. Par conséquent, la seule artère assortie dans la table de routage était le default route de retour vers le FWSM :

```
S*   0.0.0.0/0 [1/0] via 10.20.1.50
```

Le paquet a été conduit à l'**interface interne du** FWSM. La table de routage Du FWSM a indiqué que le réseau de destination de 10.40.1.0/24 a existé derrière la même **interface interne** :

```
S    10.40.1.0 255.255.255.0 [1/0] via 10.10.1.254, inside
```

Puisque la commande **intra-interface d'autorisation du même-Sécurité-trafic** est activée, le FWSM permettra le xlate u-tourné à construire.

Pour récapituler, le premier xlate a été déclenché par :

- Une large route configurée 10.0.0.0/8 sur le routeur DMZ
- **Un IP d'autorisation tout tout ACL** configuré sur l'interface interne du FWSM

Le deuxième xlate a été déclenché par :

- Une interface instable sur le routeur interne
- **intra-interface d'autorisation du même-Sécurité-trafic** configuré sur le FWSM

Solutions

Il y a beaucoup de différentes solutions au problème possibles. En premier lieu, supprimer le xlate de la table devrait permettre au trafic pour commencer fonctionner de nouveau jusqu'à ce que le xlate soit reconstruit. Ceci peut être fait avec la commande de **clear xlate**. Exemple :

```
FWSM# clear xlate interface inside local 10.30.1.1 global 10.30.1.1
```

Remarque: Toutes connexions qui utilisent supprimé

Une fois que c'est complet, le foyer devrait être sur empêcher les xlates de retourner. Souvent des périodes, la plupart de moyen privilégié de faire ceci est de réparer la configuration de routage dans l'environnement pour empêcher le trafic d'arriver sur l'interface fausse FWSM. Le FWSM offre également une poignée d'options de configuration d'aborder ces questions.

Configurations incorrectes de routage de résolution

Cette solution prend la planification rigoureuse et une compréhension profonde de l'environnement de réseau. Dans le premier exemple ci-dessus, l'artère 10.0.0.0/8 sur le routeur DMZ est techniquement incorrecte puisque le réseau entier de /8 n'existe pas au delà de son interface de 10.50.1.253. Au lieu de cela, quelques options qui existent sont :

- Éliminez 10.50.1.0/24 le réseau tous ensemble et conduisez simplement tout le trafic par le FWSM. Ceci fournit également une meilleures segmentation et Sécurité entre l'intérieur et les réseaux DMZ.
- Configurez une artère statique sur le DMZ pour seulement 10.40.1.0/24 et retirez l'artère 10.0.0.0/8.
- Employez un protocole de routage dynamique entre les Routeurs intérieurs et DMZ pour annoncer correctement seulement les réseaux qui existent réellement.

Il y a souvent beaucoup de possibilités pour ajuster la configuration de routage, mais l'objectif final est de s'assurer que le trafic d'un hôte donné peut arriver seulement sur une interface simple FWSM.

Autorisation du même-Sécurité-trafic de débronchement intra-interface

La commande **intra-interface d'autorisation du même-Sécurité-trafic** permet le FWSM à demi-tour ou au trafic d'épingle à cheveux sur une interface. Ceci signifie qu'un paquet peut entrer dans le Pare-feu sur la même interface qu'il part en fonction. Cette fonctionnalité est désactivée par défaut et a très peu d'utilisation dans la plupart des conceptions FWSM. Puisque le FWSM utilise des interfaces VLAN, trafiquez que des séjours dans le même VLAN devraient ne jamais être traités par le FWSM.

Dans le deuxième exemple ci-dessus, la commande **intra-interface d'autorisation du même-Sécurité-trafic** a permis un paquet à écrivent et partent de l'**interface interne**. Désactiver l'**autorisation du même-Sécurité-trafic intra-interface** empêcherait ce comportement et relâcherait le paquet avant qu'un xlate ait été jamais établi :

```
FWSM(config)# no same-security-traffic permit intra-interface
```

Relâchez les paquets qui arrivent sur une interface incorrecte (ACLs ou uRPF)

Dans les deux exemples ci-dessus, les xlates ont été établis quand un paquet du web server est inexactement arrivé sur l'**interface interne**. Afin d'empêcher tout le problème ensemble, le FWSM peut être configuré pour relâcher les paquets qui arrivent sur l'interface fausse.

Le FWSM exige que tout le trafic soit permis par un ACL avant qu'il puisse passer. Par conséquent, cette fonctionnalité peut être réalisée en permettant seulement le trafic des réseaux appropriés de source sur chaque interface. Dans les exemples ci-dessus, l'**interface interne** permet tout le trafic IP :

```
access-list inside_in extended permit ip any any
```

Au lieu de cela, ceci devrait être changé pour permettre seulement le trafic des 10.10.1.0/24 et 10.40.1.0/24 sous-réseaux :

```
access-list inside_in extended permit ip 10.10.1.0 255.255.255.0 any

access-list inside_in extended permit ip 10.40.1.0 255.255.255.0 any
```

Dans quelques environnements, ce n'est pas une option faisable due à la taille et/ou à l'échelle des différents réseaux traversant le FWSM. Cependant, cette fonctionnalité peut être réalisée plus simplement utilisant une caractéristique appelée le Fonction Unicast Reverse Path Forwarding (uRPF).

Quand la caractéristique d'uRPF est activée, le FWSM comparera l'adresse IP source du premier paquet de chaque connexion contre sa table de routage. Si l'artère qui est trouvée ne s'assortit pas avec l'interface que le paquet est arrivé en fonction, ce paquet sera dû lâché à une panne RPF.

Dans l'exemple ci-dessus, le FWSM a une artère statique qui emploie l'interface de **dmz** pour atteindre le réseau 10.30.1.0/24. Par conséquent, si l'uRPF est activé sur l'**interface interne**, des paquets originaires du web server (10.30.1.1) qui arrivent inexactement sur l'**interface interne** seront lâchés.

Afin d'activer l'uRPF, appliquez l'**IP vérifient la** commande de **chemin inverse à** chaque interface en question. Exemple :

```
FWSM(config)# ip verify reverse-path interface inside
```

Xlate-contournement d'enable

Dans chacun des deux exemples ci-dessus, les xlates sont créés avec les indicateurs II. Ces indicateurs indiquent que le xlate est une traduction d'identité (i) qui a commencé sur une interface de la sécurité élevée (i). Par défaut, le FWSM établira ces xlates pour n'importe quel trafic qui n'apparie pas une règle explicite NAT/PAT. Afin de désactiver ce comportement, la commande de xlate-**contournement** peut être activée dans FWSM 3.2(1) et plus tard :

```
FWSM(config)# xlate-bypass
```

Cette caractéristique empêchera le FWSM des xlates d'identité de bâtiment en premier lieu. Ainsi, le trafic dans les exemples ci-dessus ne serait pas réorienté à une interface incorrecte due à une entrée de table de xlate. Cependant, le trafic traversera toujours le FWSM non traduit.

Résumé

Afin de déterminer l'interface de sortie pour un paquet, le FWSM consultera toujours sa table de xlate avant de regarder sa table de routage. Si ce paquet apparie un xlate existant, l'interface de sortie est sélectionnée a basé sur l'interface associée des xlate. Ceci se produit indépendamment de toutes les contradictions qui pourraient être trouvées dans la table de routage. De cette façon, la table de xlate a la priorité au-dessus de la table de routage.

Puisque le FWSM établira toujours une entrée de xlate pour toutes les nouvelles connexions par défaut, ceci peut entraîner des pannes du trafic dans les cas où inexactement les paquets routés font établir le FWSM un xlate. Comme tracé les grandes lignes ci-dessus, il y a beaucoup de scénarios possibles où ceci peut se produire mais tous associent de nouveau à un paquet étant reçu sur une interface incorrecte. Ce document a couvert ces questions possibles :

- Un large config de routage envoie des paquets dans une direction incorrecte
- Le FWSM est configuré pour permettre le trafic des réseaux incorrects de source
- Le FWSM est configuré au trafic hairpin/u-turn

Afin de restaurer rapidement la Connectivité pour les connexions qui échouent en raison d'un xlate faux, supprimez l'entrée avec la commande de **clear xlate**. Ce document a également couvert de plusieurs solutions pour empêcher ces xlates de retourner à l'avenir, incluant :

- Configurations incorrectes de routage de résolution utilisant plus d'artères spécifiques
- Autorisation du même-Sécurité-trafic de débronchement intra-interface
- Relâchez les paquets qui arrivent sur une interface incorrecte utilisant ACLs ou uRPF
- Xlate-contournement d'enable

Informations connexes

- Référence de commandes : l'IP vérifient le chemin inverse
- Référence de commandes : xlate-contournement
- Support et documentation techniques - Cisco Systems