Exemple de configuration d'un pare-feu transparent dans le module de services pare-feu

Contenu

Introduction

Traditionnellement, un pare-feu est un saut de routeur qui agit en tant que passerelle par défaut pour les serveurs qui se connectent à l'un de ses sous-réseaux tramés. Un Pare-feu transparent, d'autre part, est un Pare-feu de la couche 2 que des actes comme un *bosse sur le fil* ou un *pare-feu furtif* et n'est pas vu comme saut de routeur aux périphériques connectés. Le module de service de Pare-feu (FWSM) connecte le même réseau sur ses interfaces internes et externes. Puisque le Pare-feu n'est pas un saut conduit, vous pouvez facilement introduire un Pare-feu transparent dans un réseau existant. Il n'est pas nécessaire de réadresser l'IP.

La maintenance est facilitée parce qu'il n'y a pas de modèles de routage compliqués à dépanner et aucune configuration NAT.

Quoique le mode transparent agisse en tant que passerelle, le trafic de la couche 3 (tel que le trafic IP) ne peut pas traverser le FWSM à moins que vous le permettiez explicitement avec une liste d'accès étendue. Le seul trafic permis à travers le pare-feu transparent sans liste d'accès est le trafic ARP. Le trafic ARP peut être contrôlé par l'inspection ARP.

En mode conduit, quelques types de trafic ne peuvent pas traverser le FWSM même si vous le permettez dans une liste d'accès. Alternativement, le pare-feu transparent peut autoriser tout trafic à travers une liste d'accès étendue (pour le trafic IP) ou une liste d'accès EtherType (pour le trafic non-IP).

Par exemple, vous pouvez établir des contiguïtés de protocole de routage par un Pare-feu transparent. vous pouvez permettre le trafic VPN (IPSec), OSPF, RIP, EIGRP ou BGP sur la base d'une liste d'accès étendue. De même, les protocoles tels que le HSRP ou le VRRP peuvent traverser le FWSM.

Le trafic non-IP (par exemple, AppleTalk, IPX, BPDUs et MPLS) peut être configuré pour aller de pair avec une liste d'accès EtherType.

Pour les caractéristiques qui ne sont pas directement prises en charge sur le pare-feu transparent, vous pouvez laisser le trafic passer de façon à ce que les routeurs en amont et en aval puissent prendre en charge la fonctionnalité. Par exemple, avec une liste d'accès étendue, vous pouvez autoriser le trafic DHCP (au lieu de la fonctionnalité de relais DHCP non prise en charge) ou le trafic de multidiffusion, comme celui créé par IP/TV.

Quand le FWSM fonctionne en mode transparent, l'interface sortante d'un paquet est déterminée par une consultation d'adresse MAC au lieu d'une recherche de route. Des instructions de route peuvent encore être configurées, mais elles s'appliquent seulement au trafic FWSM-d'origine. Par exemple, si votre serveur de Syslog se trouve sur un réseau distant, vous devez utiliser une artère statique, ainsi le FWSM peut atteindre ce sous-réseau.

Une exception à la règle est quand vous utilisez des inspections de Voix et le point final est au moins un saut à partir du FWSM. Par exemple, si vous utilisez le Pare-feu transparent entre un CCM et une passerelle H.323, et il y a un routeur entre le Pare-feu transparent et la passerelle H.323, puis vous devez ajouter une artère statique sur le FWSM pour la passerelle H.323 pour la fin réussie d'appel.

Remarque: Le mode transparent FWSM ne passe les paquets de CDP ou aucun paquet qui n'ont pas un EtherType supérieur ou égal à un 0x600 valides. Par exemple, vous ne pouvez pas passer des paquets IS-IS. Une exception est faite pour les BPDU, qui sont pris en charge.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur FWSM avec la version 3.x.

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.

Conventions

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

Pare-feu transparent

Groupes de passerelle

Si vous ne voulez pas le temps système des contextes de sécurité, ou voulez maximiser votre utilisation des contextes de sécurité, vous pouvez configurer jusqu'à huit paires d'interfaces, appelées des groupes de passerelle. Chaque groupe de passerelle se connecte à un réseau indépendant. Le trafic de groupe de passerelle est isolé dans d'autres groupes de passerelle. Le trafic n'est pas conduit à un autre groupe de passerelle dans le FWSM, et le trafic doit quitter le FWSM avant qu'il soit conduit par un routeur externe de nouveau à un autre groupe de passerelle dans le FWSM. Bien que les fonctions traversières soient distinctes pour chaque groupe de passerelle, beaucoup d'autres fonctions sont partagées entre tous les groupes de passerelle. Par exemple, tous les groupes de passerelle partagent un serveur de log système ou une configuration du serveur d'AAA. Pour la séparation complète de stratégie de sécurité, contextes de sécurité d'utilisation avec un groupe de passerelle dans chaque contexte.

Puisque le Pare-feu n'est pas un saut conduit, vous pouvez facilement introduire un Pare-feu transparent dans un réseau existant. Il n'est pas nécessaire de réadresser l'IP. La maintenance est facilitée parce qu'il n'y a pas de modèles de routage compliqués à dépanner et aucune configuration NAT.

Remarque: Chaque groupe de passerelle exige une adresse IP de Gestion. Le FWSM utilise cette adresse IP comme adresse source pour les paquets qui proviennent du groupe de passerelle. L'adresse IP de gestion doit être sur le même sous-réseau que le réseau connecté.

Instructions

Suivez ces instructions quand vous planifiez votre réseau de pare-feu transparent :

- Une adresse IP de Gestion est exigée pour chaque groupe de passerelle.Àla différence du mode conduit, qui exige une adresse IP pour chaque interface, un Pare-feu transparent a une adresse IP assignée au groupe entier de passerelle. Le FWSM utilise cette adresse IP comme adresse source pour les paquets qui commencent sur le FWSM, tel que des messages système ou des transmissions d'AAA.L'adresse IP de gestion doit être sur le même sous-réseau que le réseau connecté. Vous ne pouvez pas configurer le sous-réseau sur un réseau interne (255.255.255.255). Le FWSM ne prend en charge pas le trafic sur les réseaux secondaires ; trafiquez seulement sur le même réseau que l'adresse IP de Gestion est pris en charge. Référez-vous à assigner une adresse IP à un groupe de passerelle pour plus d'informations sur des sous-réseaux IP de Gestion.
- Chaque groupe de passerelle utilise une interface interne et une interface extérieure

seulement.
- Chaque réseau directement connecté doit être sur le même sous-réseau.
- Ne spécifiez pas l'adresse IP de Gestion de groupe de passerelle comme passerelle par défaut pour des périphériques connectés. Les périphériques doivent spécifier le routeur de l'autre côté du FWSM comme passerelle par défaut.
- Le default route pour le Pare-feu transparent, qui est exigé pour fournir un chemin de retour pour le trafic d'administration, est seulement appliqué au trafic d'administration à partir d'un réseau de groupe de passerelle. C'est parce que le default route spécifie une interface dans le groupe de passerelle aussi bien que l'adresse IP du routeur sur le réseau de groupe de passerelle, et vous pouvez seulement définir un default route. Si vous avez le trafic d'administration de plus d'un réseau de groupe de passerelle, vous devez spécifier une artère statique qui identifie le réseau dont vous vous attendez au trafic d'administration.
- Pour le mode de contexte multiple, chaque contexte doit utiliser différentes interfaces. Vous ne pouvez pas partager d'interface à travers des contextes.
- Pour le mode de contexte multiple, chaque contexte utilise typiquement des différents sous-réseaux. Vous pouvez utiliser des sous-réseaux superposants, mais votre topologie du réseau exige du routeur et de la configuration NAT de la rendre possible à partir d'un point de vue de routage.Vous devez employer une liste d'accès étendue pour permettre le trafic de la couche 3, tel que le trafic IP, par le FWSM. Vous pouvez également utiliser en option une liste d'accès EtherType pour permettre le passage du trafic non-IP.

Adresses MAC autorisées

Ces adresses MAC de destination ont la permission de passer à travers le pare-feu transparent. Toute adresse MAC ne figurant pas sur cette liste est abandonnée.

- L'adresse MAC de destination de VÉRITABLE diffusion équivaut à FFFF.FFFF.FFFF
- Addresses MAC multicast Ipv4 de 0100.5E00.0000 à 0100.5EFE.FFFF
- Addresses MAC multicast Ipv6 de 3333.0000.0000 à 3333.FFFF.FFFF
- L'adresse multicast BPDU est égale à 0100.0CCC.CCCD
- Adresses MAC multicast AppleTalk de 0900.0700.0000 à 0900.07FF.FFFF

Fonctions non prises en charge

Ces fonctions ne sont pas prises en charge en mode transparent :

- NAT /PATNAT est exécuté sur le routeur en amont.**Remarque:** NAT/PAT est pris en charge dans le Pare-feu transparent pour des versions de version 3.2 et ultérieures FWSM.
- Protocoles de routage dynamique (tels que la RIP, EIGRP, OSPF)Vous pouvez ajouter les artères statiques pour le trafic qui commence sur le FWSM. Vous pouvez également permettre des protocoles de routage dynamique par le FWSM avec une liste d'accès étendue.
- IPv6 pour l'adresse IP de groupe de passerelle.Cependant, vous pouvez passer l'IPv6 EtherType utilisant une liste d'accès d'EtherType.
- Relais DHCPLe pare-feu transparent peut agir en tant que serveur DHCP, mais il ne prend pas en charge les commandes de relais DHCP. Le relais DHCP n'est pas nécessaire parce que vous pouvez permettre le passage du trafic DHCP à travers une liste d'accès étendue.
- Qualité de service (QoS)
- MultidiffusionVous pouvez permettre le trafic de multidiffusion par le FWSM si vous le

permettez dans une liste d'accès étendue. Référez-vous au pour en savoir plus de section du trafic de traverser.

- Terminaison VPN pour le passage du traficLe pare-feu transparent prend en charge des tunnels VPN de site-à-site pour des connexions de gestion seulement. Il ne termine pas des connexions VPN pour le trafic par le FWSM. Vous pouvez passer le trafic VPN par le FWSM avec une liste d'accès étendue, mais elle ne termine pas des connexions de non-Gestion.
- LoopGuard sur le commutateurN'activez pas LoopGuard globalement sur le commutateur si le FWSM est en mode transparent. LoopGuard est automatiquement appliqué à l'EtherChannel interne entre le commutateur et le FWSM, ainsi après un Basculement et une restauration, LoopGuard cause l'unité secondaire d'être déconnectée parce que l'EtherChannel entre dans l'état d'errer-débronchement.

Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Le schéma de réseau montre un réseau de pare-feu transparent général où les périphériques externes sont sur le même sous-réseau que les périphériques internes. Le routeur interne et les serveurs semblent être directement connectés au routeur externe.

Configurations

Vous pouvez placer chaque contexte pour s'exécuter en mode conduit de Pare-feu (le par défaut) ou mode transparent de Pare-feu.

Quand vous changez des modes, le FWSM efface la configuration parce que beaucoup de commandes ne sont pas prises en charge pour les deux modes. Si vous avez déjà une configuration remplie, soyez sûr de sauvegarder votre configuration avant que vous changiez le mode. Vous pouvez utiliser cette sauvegarde pour la référence en créant votre nouvelle configuration.

Si vous téléchargez une configuration des textes au FWSM qui change le mode avec la commande transparente de Pare-feu, soyez sûr de mettre la commande en haut de la configuration. Le FWSM change le mode dès qu'il lira la commande et puis continue de lire la configuration que vous avez téléchargée. Si la commande est plus tard dans la configuration, le FWSM efface toutes les lignes précédentes dans la configuration.

Afin de placer le mode à transparent, sélectionnez cette commande dans chaque contexte :

```
hostname(config)#firewall transparent
```

Afin de placer le mode à conduire, sélectionnez cette commande dans chaque contexte :

```
hostname(config)#no firewall transparent
```

Les données se déplacent à travers le pare-feu transparent dans différents scénarios

Un utilisateur interne accède au serveur d'e-mail externe

L'utilisateur sur le réseau interne accède au serveur d'e-mail placé dans Internet (à l'extérieur). Le FWSM reçoit le paquet et ajoute l'adresse MAC source à la table d'adresse MAC, s'il y a lieu. Puisqu'il s'agit d'une nouvelle session, il vérifie que le paquet est autorisé selon les termes de la politique de sécurité (listes d'accès, filtres ou AAA).

Remarque: Pour le mode de contexte multiple, le FWSM classifie d'abord le paquet selon une seule interface.

Le FWSM enregistre qu'une session est établie. Si l'adresse MAC de destination est dans sa table, le FWSM en avant le paquet hors de l'interface extérieure. L'adresse de destination MAC est celle du routeur en amont, 192.168.1.2. Si l'adresse MAC de destination n'est pas dans la table FWSM, les tentatives FWSM de découvrir l'adresse MAC quand elle envoie une demande d'ARP et un ping. Le premier paquet est lâché.

Le serveur de mail répond à la demande. Parce que la session est déjà établie, le paquet saute les nombreuses recherches associées à un nouvelle connexion. Le FWSM en avant le paquet à l'utilisateur intérieur.

Un utilisateur intérieur visite un serveur de mail avec NAT

Si vous activez NAT sur le routeur Internet, le flux du paquet à travers le routeur Internet est légèrement changé.

L'utilisateur sur le réseau interne accède au serveur d'e-mail placé dans Internet (à l'extérieur). Le FWSM reçoit le paquet et ajoute l'adresse MAC source à la table d'adresse MAC, s'il y a lieu. Puisqu'il s'agit d'une nouvelle session, il vérifie que le paquet est autorisé selon les termes de la politique de sécurité (listes d'accès, filtres ou AAA).

Remarque: Pour le mode de contexte multiple, le FWSM classifie d'abord le paquet selon une seule interface.

Le routeur Internet traduit l'adresse réelle de l'hôte A (192.168.1.5) à l'adresse mappée du routeur Internet (172.16.1.1). Puisque l'adresse tracée n'est pas sur le même réseau que l'interface extérieure, assurez-vous que le routeur en amont a une artère statique au réseau tracé ces points au FWSM.

Le FWSM enregistre qu'une session est établie et en avant le paquet de l'interface extérieure. Si l'adresse MAC de destination est dans sa table, le FWSM en avant le paquet hors de l'interface extérieure. L'adresse de destination MAC est celle du routeur en amont, 172.16.1.1. Si l'adresse MAC de destination n'est pas dans la table FWSM, les tentatives FWSM de découvrir l'adresse MAC quand elle envoie une demande d'ARP et un ping. Le premier paquet est lâché.

Le serveur de mail répond à la demande. Parce que la session est déjà établie, le paquet saute les nombreuses recherches associées à un nouvelle connexion. Le FWSM exécute NAT quand il traduit l'adresse tracée à la vraie adresse, 192.168.1.5.

Un utilisateur interne visite un serveur Web interne

Si les essais de l'hôte A pour accéder au web server intérieur (10.1.1.1), hébergent A (192.168.1.5) envoie le paquet de demandes au routeur internet (puisque c'est une passerelle par défaut) par le FWSM de l'intérieur à l'extérieur. Alors le paquet est réorienté au web server (10.1.1.1) par FWSM (externe vers interne) et le routeur interne.

Remarque: Le paquet de demandes revient au web server seulement si le FWSM a une liste d'accès pour permettre le trafic de l'extérieur à l'intérieur.

Afin de résoudre ce problème, changez la passerelle par défaut pour l'hôte A (10.1.1.1) pour être le routeur interne (192.168.1.3) au lieu du routeur internet (192.168.1.2). Ceci évite tout trafic inutile envoyé à la passerelle externe et redirige des occurrences sur le routeur externe (routeur Internet). Il résout également dans le sens inverse, c.-à-d., quand le serveur Web ou tout hôte présent (10.1.1.0/24) à l'intérieur du routeur interne essaie d'accéder à l'Hôte A (192.168.1.5).

Un utilisateur externe visite un serveur Web sur le réseau interne

Ces étapes décrivent comment les données se déplacent par le FWSM :

1. Un utilisateur sur le réseau externe demande une page Web du serveur Web interne. Le FWSM reçoit le paquet et ajoute l'adresse MAC source à la table d'adresse MAC, s'il y a lieu. Puisqu'il s'agit d'une nouvelle session, il vérifie que le paquet est autorisé selon les termes de la politique de sécurité (listes d'accès, filtres ou AAA).**Remarque:** Pour le mode de contexte multiple, le FWSM classifie d'abord le paquet selon une seule interface.
2. Le FWSM enregistre qu'une session est établie seulement si l'utilisateur externe a l'accès valide au web server interne. La liste d'accès doit être configurée pour permettre à l'utilisateur externe d'avoir accès au serveur Web.
3. Si l'adresse MAC de destination est dans sa table, le FWSM en avant le paquet hors de l'interface interne. L'adresse de destination MAC est celle du routeur en aval, 192.168.1.3.
4. Si l'adresse MAC de destination n'est pas dans la table FWSM, les tentatives FWSM de découvrir l'adresse MAC quand elle envoie une demande d'ARP et un ping. Le premier paquet est lâché.
5. Le web server répond à la demande. Parce que la session est déjà établie, le paquet saute les nombreuses recherches associées à un nouvelle connexion. Le FWSM en avant le paquet à l'utilisateur externe.

Un utilisateur externe essaie d'accéder à un hôte interne

Un utilisateur sur le réseau externe essaie d'atteindre un hôte interne. Le FWSM reçoit le paquet et ajoute l'adresse MAC source à la table d'adresse MAC, s'il y a lieu. Puisqu'il s'agit d'une nouvelle session, il vérifie que le paquet est autorisé selon les termes de la politique de sécurité (listes d'accès, filtres ou AAA).

Remarque: Pour le mode de contexte multiple, le FWSM classifie d'abord le paquet selon une seule interface.

Le paquet est refusé, et le FWSM relâche le paquet parce que l'utilisateur externe n'a pas l'accès à l'hôte interne. Si les tentatives d'utilisateur externe d'attaquer le réseau intérieur, le FWSM utilise beaucoup de Technologies pour déterminer si un paquet est valide pour une session déjà établie.

Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

```
cisco(config)#show firewall Firewall mode: Transparent
```

Dépannez

Traversez le trafic

Dans le Pare-feu transparent, pour passer le trafic de multidiffusion de haut en bas et le bas aux Listes d'accès élevées sont exigés. Dans des Pare-feu normaux de haut en bas n'est pas exigé.

Remarque: On ne laissera pas l'adresse de multidiffusion (224.0.0.9) peut ne jamais être adresse source pour le trafic de retour, ainsi lui revenir dedans, qui est pourquoi nous avons besoin des ACL de dedans à et à dedans.

Par exemple, afin de traverser le trafic de déchirure, la liste d'accès transparente de Pare-feu serait semblable à cet exemple :

RIP

ACL extérieur (de à dedans) :

```
access-list outside permit udp host (outside source router) host 224.0.0.9 eq 520
access-group outside in interface outside
```

ACL intérieur (de l'intérieur de à l'extérieur) :

```
access-list inside permit udp host (inside source router) host 224.0.0.9 eq 520
access-group inside in interface inside
```

EIGRP à s'exécuter :

```
access-list inside permit eigrp host (inside source) host 224.0.0.10
 access-group inside in interface inside
access-list outside permit eigrp host (outside source) host 224.0.0.10
access-group outside in interface outside
```

Pour l'OSPF :

```
access-list inside permit ospf host ( inside source ) host 224.0.0.5
( this access-list is for hello packets )
access-list inside permit ospf host ( inside source ) host 224.0.0.6
( dr send update on this port )
access-list inside permit ospf host ( inside source ) host ( outside source )
access-group inside in interface inside
 access-list outside permit ospf host ( outside source ) host 224.0.0.5
access-list outside permit ospf host ( outside source ) host 224.0.0.6
access-list outside permit ospf host ( outside sourec ) host ( inside source )
access-group outside in interafce outside
```

MSFC VLAN contre FWSM VLAN

En mode transparent, il n'est pas nécessaire d'avoir les mêmes VLAN dans l'interface MSFC et le FWSM, puisque c'est un type de transition.

Informations connexes

- Logiciels pare-feu Cisco PIX
- Demandes de commentaires (RFC)
- Notices de champs relatives aux produits de sécurité (y compris PIX)
- Références des commandes du pare-feu Cisco Secure PIX
- PIX/ASA : Exemple de configuration d'un pare-feu transparent
- Support et documentation techniques - Cisco Systems