ASA/PIX : Exemple de configuration d'autorisation du trafic réseau à accéder à Microsoft Media Server (MMS) et à des flux vidéo à partir d'Internet

Contenu

Introduction

Ce document décrit comment configurer l'appliance de sécurité adaptable (ASA) dans la commande l'autoriser le client ou l'utilisateur de l'Internet pour accéder à la Microsoft Media Server (MMS) ou le streaming vidéo a placé dans le réseau intérieur de l'ASA.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Configuration de base d'ASA
- Le MMS est configuré et fonctionne correctement

Composants utilisés

Les informations dans ce document sont basées sur Cisco ASA qui exécute la version de logiciel 7.x et plus tard.

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.

Produits connexes

Les informations dans ce document s'appliquent également au Pare-feu de Cisco PIX qui exécute la version de logiciel 7.x et plus tard.

Conventions

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

Les informations de Pare-feu pour la gamme 9 de services de Windows Media

Protocoles de streaming media d'utilisation

Le ® de Windows Media de ® de Microsoft entretient des utilisations de gamme 9 deux protocoles coulants de medias de fournir le contenu comme flot d'unicast aux clients :

- Protocole RTSP (Real-Time Streaming Protocol)
- Protocole de la Microsoft Media Server (MMS)

Ces protocoles prennent en charge des actions de contrôle de client telles que l'arrêt, font une pause, rembobinent, et se déroulent en avance rapide les fichiers de Windows Media répertoriés.

Le RTSP est un protocole de la couche applicative qui a été créé spécifiquement pour fournir la livraison commandée des données en temps réel, telles que le contenu audio et vidéo. Vous pouvez employer le RTSP pour couler le contenu aux ordinateurs qui exécutent la gamme 9 de Lecteur Windows Media ou plus tard, aux clients qui utilisent le contrôle de ® d'ActiveX de gamme 9 de Lecteur Windows Media, ou à d'autres ordinateurs qui exécutent la gamme 9 de services de Windows Media. Le RTSP fonctionne en tandem avec le Protocole RTP (Real-Time Transport Protocol) pour formater des paquets de contenu multimédia et pour négocier le protocole de la couche transport le plus efficace, Protocole UDP (User Datagram Protocol) ou Control Protocol de transport (TCP), pour l'utiliser quand vous livrez le flot aux clients. Vous pouvez implémenter le RTSP par le périphérique prêt à brancher de Control Protocol de serveur de RTSP WMS dans l'administrateur de services de Windows Media. Ce périphérique prêt à brancher est activé par défaut.

Le MMS est un protocole de la couche applicative de propriété industrielle qui a été développé pour des versions antérieures des services de Windows Media. Vous pouvez employer le MMS pour couler le contenu aux ordinateurs qui exécutent des Windows Media Player pour le XP de ®

de Windows ou plus tôt. Vous pouvez implémenter le MMS par le périphérique prêt à brancher de Control Protocol de serveur WMS MMS dans l'administrateur de services de Windows Media. Ce périphérique prêt à brancher est activé par défaut.

HTTP d'utilisation

Si des ports sur votre Pare-feu ne peuvent pas être ouverts, les services de ® de Windows Media peuvent couler le contenu avec le HTTP au-dessus du port 80. Le HTTP peut être utilisé pour livrer des flots à toutes les versions de Windows Media Player. Vous pouvez implémenter le HTTP par le périphérique prêt à brancher de Control Protocol de serveur HTTP WMS dans l'administrateur de services de Windows Media. Ce périphérique prêt à brancher n'est pas activé par défaut. Si un autre service, tel que l'Internet Information Services (IIS), utilise le port 80 sur la même adresse IP, vous ne pouvez pas activer le périphérique prêt à brancher.

Le HTTP peut également être utilisé pour ces derniers :

- Distribuez les flots entre les serveurs de Windows Media
- Contenu de source d'un encodeur de Windows Media
- Listes d'écoute dynamiquement générées de téléchargement d'un serveur Web

Des connexions de point d'émission de données doivent être configurées dans l'administrateur de services de Windows Media pour prendre en charge ces HTTP supplémentaire coulant des scénarios.

Au sujet du renversement de Protocol

Si les clients qui prennent en charge le RTSP se connectent à un serveur qui dirige des services de ® de Windows Media avec un surnom URL de RTSP (par exemple, rtsp://) ou un surnom URL MMS (par exemple, mms://), le serveur emploie le renversement de protocole pour couler le contenu au client pour fournir une expérience coulante optimale. Le renversement automatique de protocole de RTSP/MMS au RTSP avec les transports basés sur UDP ou basés sur TCP (RTSPU ou RTSPT), ou même le HTTP (si le périphérique prêt à brancher de Control Protocol de serveur HTTP WMS est activé) peut se produire comme essais de serveur pour négocier le meilleur protocole et pour fournir une expérience coulante optimale pour le client. Les clients qui prennent en charge le RTSP incluent la gamme 9 de Lecteur Windows Media ou plus tard ou d'autres lecteurs qui utilisent le contrôle d'ActiveX de gamme 9 de Lecteur Windows Media.

Les versions antérieures des Windows Media Player, telles que des Windows Media Player pour Windows XP, ne prennent en charge pas le protocole de RTSP, mais le protocole MMS fournit le support inversé de protocole pour ces clients. Ainsi, quand une version antérieure des tentatives de lecteur de se connecter au serveur à un surnom URL MMS, à un renversement automatique de protocole de MMS au MMS aux transports basés sur UDP ou basés sur TCP (MMSU ou MMST), ou même à un HTTP (si le périphérique prêt à brancher de Control Protocol de serveur HTTP WMS est activé), peut se produire comme essais de serveur pour négocier le meilleur protocole et fournir une expérience coulante optimale pour ces clients.

Afin de s'assurer que votre contenu est à la disposition de tous les clients qui se connectent à votre serveur, des ports sur votre Pare-feu doivent être ouverts pour tous les protocoles de connexion qui peuvent être utilisés dans le renversement de protocole.

Vous pouvez forcer votre serveur de Windows Media pour utiliser un protocole spécifique si vous identifiez le protocole à utiliser dans le fichier d'annonce (par exemple,

rtspu://server/publishing_point/file). Afin de fournir une expérience coulante optimale pour toutes les versions du client, nous recommandons que l'utilisation URL le protocole du général MMS. Si les clients se connectent à votre flot à un URL à un surnom URL MMS, n'importe quel renversement nécessaire de protocole se produit automatiquement. Rendez-vous compte que les utilisateurs peuvent désactiver des Protocoles de diffusion en flux dans les configurations de propriété des Windows Media Player. Si un utilisateur désactive un protocole, il est ignoré dans le renversement. Par exemple, si le HTTP est désactivé, l'URLs ne roulent pas plus d'au HTTP.

Allouez les ports pour des services de Windows Media

La plupart des Pare-feu sont utilisés pour contrôler « le trafic d'arrivée » au serveur ; ils généralement ne contrôlent pas le « trafic sortant » aux clients. Les ports dans votre Pare-feu pour le trafic sortant peuvent être fermés si une stratégie de sécurité plus rigoureuse est mise en application sur votre réseau serveur. Cette section décrit l'allocation par défaut de port pour des services de ® de Windows Media pour des les deux le trafic en entrée et en sortie (affiché en tant que « dans » et « » dans les tables) de sorte que vous puissiez configurer tous les ports comme nécessaires.

Dans quelques scénarios, le trafic sortant peut être dirigé vers un port dans une plage des ports disponibles. Les chaînes de port affichées dans les tables indiquent la plage entière des ports disponibles, mais vous pouvez allouer moins ports dans la marge de port. Quand vous décidez combien de ports pour s'ouvrir, Sécurité d'équilibre avec l'accessibilité et pour ouvrir de juste assez de ports pour permettre à tous les clients pour établir un rapport. D'abord, déterminez combien de ports vous comptez utiliser pour les services de Windows Media, et ouvrir alors 10 pour cent de plus pour expliquer la superposition avec d'autres programmes. Après que vous ayez établi ce nombre, surveillez votre trafic pour déterminer si des réglages sont nécessaires.

Les restrictions de chaîne de port affectent potentiellement tout le protocole RPC (RPC) et applications composantes réparties du modèle objet (DCOM) qui partagent le système, pas simplement des services de Windows Media. Si la plage allouée de port n'est pas assez large, les services concurrentiels tels qu'IIS peuvent échouer avec des erreurs aléatoires. La plage de port doit pouvoir faciliter toutes les applications système potentielles qui utilisent des services RPC, COM, ou DCOM.

Afin de faciliter la configuration de Pare-feu, vous pouvez configurer chaque périphérique prêt à brancher de protocole de contrôle de serveur (RTSP, MMS, et HTTP) dans l'administrateur de services de Windows Media pour utiliser un port spécifique. Si votre administrateur réseau a déjà ouvert une gamme de ports à l'usage de vos Windows Media serveur, vous pouvez allouer ces ports aux protocoles de contrôle en conséquence. Sinon, vous pouvez demander à l'administrateur réseau d'ouvrir les ports par défaut pour chaque protocole. S'il n'est pas possible aux ports ouverts sur votre Pare-feu, les services de Windows Media peuvent couler le contenu avec le protocole HTTP au-dessus du port 80.

C'est l'allocation par défaut de port de Pare-feu pour des services de Windows Media afin de livrer un flot d'unicast :

Protocole de l'application	Protocol	Port	Description
RTSP	TC	554	Utilisé pour recevoir les connexions

	P	(entrée/sortie)	client d'arrivée de RTSP et pour livrer des paquets de données aux clients qui coulent avec RTSPT.
RTSP	UDP	5004 ()	Utilisé pour livrer des paquets de données aux clients qui coulent avec RTSPU.
RTSP	UDP	5005 (entrée/sortie)	Utilisé pour recevoir les informations de perte de paquets des clients et pour fournir des informations de synchronisation aux clients qui coulent avec RTSPU.
MMS	TCP	1755 (entrée/sortie)	Utilisé pour recevoir les connexions client d'arrivée MMS et pour livrer des paquets de données aux clients qui coulent avec MMST.
MMS	UDP	1755 (entrée/sortie)	Utilisé pour recevoir les informations de perte de paquets des clients et pour fournir des informations de synchronisation aux clients qui coulent avec MMSU.
MMS	UDP	1024-5000 ()	Utilisé pour livrer des paquets de données aux clients qui coulent avec MMSU. Ouvrez seulement le nombre nécessaire de ports.
HTTP	TCP	80 (entrée/sortie)	Utilisé pour recevoir les connexions client d'arrivée de HTTP et pour livrer des paquets de données aux clients qui coulent avec le HTTP.

Afin de s'assurer que votre contenu est disponible à toutes les versions du client qui se connectent à votre serveur, ouvrez tous les ports décrits dans la table pour tous les protocoles de connexion qui peuvent être utilisés dans le renversement de protocole. Si vous dirigez des services de Windows Media sur un ordinateur qui exécute Windows Server™ 2003 Service Pack 1 (SP1), vous devez ajouter le programme de services de Windows Media (wmserver.exe) comme exception dans le pare-feu Windows pour ouvrir les ports d'arrivée par défaut pour l'unicast coulant, plutôt que des ports ouverts dans le Pare-feu manuellement.

Remarque: Référez-vous au site Web de Microsoft afin de connaître plus la configuration de Pare-feu MMS.

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

Ce document utilise la configuration réseau suivante :

Remarque: Les schémas d'adressage d'IP utilisés dans cette configuration ne sont pas légalement routables sur Internet. Ce sont des adresses RFC 1918 qui ont été utilisées dans un environnement de laboratoire.

Configurations

Ce document utilise les configurations suivantes :

Configuration ASA

```
CiscoASA#Show running-config : Saved : ASA Version
8.0(2) ! hostname ciscoasa enable password
8Ry2YjIyt7RRXU24 encrypted names ! interface Ethernet0/0
nameif outside security-level 0 ip address 192.168.1.2
255.255.255.0 ! interface Ethernet0/1 nameif inside
security-level 100 ip address 10.1.1.1 255.255.255.0 !
!--- Output suppressed access-list outside_access_in
extended permit icmp any any access-list
outside_access_in extended permit udp any host
192.168.1.5 eq 1755 !--- Command to open the MMS udp
port access-list outside_access_in extended permit tcp
any host 192.168.1.5 eq 1755 !--- Command to open the
MMS tcp port access-list outside_access_in extended
permit udp any host 192.168.1.5 eq 5005 !--- Command to
open the RTSP udp port access-list outside_access_in
extended permit tcp any host 192.168.1.5 eq www !---
Command to open the HTTP port access-list
outside_access_in extended permit tcp any host
192.168.1.5 eq rtsp !--- Command to open the RTSP tcp
port !--- Output suppressed static (inside,outside)
192.168.1.5 10.1.1.5 netmask 255.255.255.255 !---
Translates the mapped IP 192.168.1.5 to the translated
IP 10.1.1.5 of the MMS. access-group outside_access_in
in interface outside !--- Output suppressed telnet
timeout 5 ssh timeout 5 console timeout 0 threat-
detection basic-threat threat-detection statistics
access-list ! class-map inspection_default match
default-inspection-traffic ! ! policy-map type inspect
dns preset_dns_map parameters message-length maximum 512
policy-map global_policy class inspection_default
inspect dns preset_dns_map inspect ftp inspect h323 h225
inspect h323 ras inspect netbios inspect rsh inspect
rtsp !--- RTSP inspection is enabled by default inspect
skinny inspect esmtp inspect sqlnet inspect sunrpc
inspect tftp inspect sip inspect xdmcp ! service-policy
global_policy global
```

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** .

- **Liste d'accès d'exposition** — Affiche l'ACLs configuré dans l'ASA/PIX`ciscoASA#show access-list access-list outside_access_in; 6 elements access-list outside_access_in line 1 extended`

```
permit icmp any any (hitcnt=0) 0x71af81e1 access-list outside_access_in line 2 extended
permit udp any host 192.168.1.5 eq 1755 (hitcnt=0) 0x4 2606263 access-list outside_access_in
line 3 extended permit tcp any host 192.168.1.5 eq 1755 (hitcnt=0) 0xa 0161e75 access-list
outside_access_in line 4 extended permit udp any host 192.168.1.5 eq 5005 (hitcnt=0) 0x3
90e9949 access-list outside_access_in line 5 extended permit tcp any host 192.168.1.5 eq www
(hitcnt=0) 0xe5 db0efc access-list outside_access_in line 6 extended permit tcp any host
192.168.1.5 eq rtsp (hitcnt=0) 0x5 6fa336f
```

- **Exposition nat** — Stratégies NAT et compteurs d'affichages.`ciscoASA(config)#`**`show nat`** `NAT policies on Interface inside: match ip inside host 10.1.1.5 outside any static translation to 192.168.1.5 translate_hits = 0, untranslate_hits = 0`

Couler VideoTroubleshoot

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Examinez le RTSP est une configuration par défaut sur l'ASA. Il casse le trafic MMS puisque les dispositifs de sécurité ne peuvent pas exécuter NAT sur des messages de RTSP parce que les adresses IP incluses sont contenues dans les fichiers SDP en tant qu'élément des messages de HTTP ou de RTSP. Des paquets peuvent être fragmentés, et les dispositifs de sécurité ne peuvent pas exécuter NAT sur les paquets fragmentés.

Contournement : Ce problème peut être résolu si vous désactivez l'inspection de RTSP pour ce trafic particulier MMS comme affiché :

```
access-list rtsp-acl extended deny tcp
   any host 192.168.1.5 eq 554
access-list rtsp-acl extended permit tcp any any eq 554
class-map rtsp-traffic
match access-list rtsp-acl
policy-map global_policy
class inspection_default
no inspect rtsp
class rtsp-traffic
inspect rtsp
```

Informations connexes

- Logiciels pare-feu Cisco PIX
- Références des commandes du pare-feu Cisco Secure PIX
- Notices de champs relatives aux produits de sécurité (y compris PIX)
- Demandes de commentaires (RFC)
- Support technique - Cisco Systems
- Page de support de Cisco ASA
- Support et documentation techniques - Cisco Systems