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'appareil de sécurité adaptatif (ASA) afin de permettre au client ou à l'utilisateur d'Internet d'accéder à Microsoft Media Server (MMS) ou à la vidéo en continu placée dans le réseau interne d'ASA.

Conditions préalables

Conditions requises

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

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

Components Used

Les informations contenues dans ce document sont basées sur Cisco ASA qui exécute les versions 7.x et ultérieures du logiciel.

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.

Produits connexes

Les informations de ce document s'appliquent également au pare-feu Cisco PIX Firewall qui exécute Software Version 7.x et ultérieure.

Conventions

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

Informations sur le pare-feu pour la gamme Windows Media Services 9

Utiliser les protocoles de diffusion multimédia en continu

La gamme Microsoft® Windows Media® Services 9 utilise deux protocoles de diffusion multimédia en continu pour transmettre du contenu sous forme de flux monodiffusion aux clients :

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

Ces protocoles prennent en charge les actions de contrôle client telles que les fichiers Windows Media indexés à progression rapide, tels que les fichiers d'arrêt, de pause, de rembobinage et de transfert rapide.

RTSP est un protocole de couche application créé spécifiquement pour fournir une livraison contrôlée de données en temps réel, telles que du contenu audio et vidéo. Vous pouvez utiliser RTSP pour diffuser du contenu vers des ordinateurs exécutant Windows Media Player 9 ou version ultérieure, vers des clients qui utilisent le contrôle ActiveX® du Lecteur Windows Media 9 ou vers d'autres ordinateurs exécutant Windows Media Services 9. RTSP fonctionne en tandem avec le protocole RTP (Real-Time Transport Protocol) pour formater les paquets de contenu multimédia et négocier le protocole de couche transport le plus efficace, UDP (User Datagram Protocol) ou TCP (Transport Control Protocol), à utiliser lors de la transmission du flux aux clients. Vous pouvez implémenter RTSP via le plug-in WMS RTSP Server Control Protocol dans l'administrateur des services Windows Media. Ce plug-in est activé par défaut.

MMS est un protocole de couche application propriétaire développé pour les versions antérieures de Windows Media Services. Vous pouvez utiliser MMS pour diffuser du contenu sur des ordinateurs qui exécutent le Lecteur Windows Media pour Windows® XP ou une version antérieure. Vous pouvez mettre en oeuvre MMS via le plug-in WMS MMS Server Control Protocol dans l'Administrateur des services Windows Media. Ce plug-in est activé par défaut.

Utiliser HTTP

Si les ports de votre pare-feu ne peuvent pas être ouverts, Windows Media® Services peut diffuser du contenu avec HTTP sur le port 80. HTTP peut être utilisé pour transmettre des flux à toutes les versions du Lecteur Windows Media. Vous pouvez implémenter HTTP via le plug-in WMS HTTP Server Control Protocol dans l'Administrateur des services Windows Media. Ce plug-in n'est pas activé par défaut. Si un autre service, tel qu'Internet Information Services (IIS), utilise le port 80 sur la même adresse IP, vous ne pouvez pas activer le plug-in.

HTTP peut également être utilisé pour les éléments suivants :

- Distribuer les flux entre les serveurs Windows Media
- Contenu source d'un encodeur Windows Media
- Télécharger des listes de lecture générées dynamiquement à partir d'un serveur Web

Les plug-ins de source de données doivent être configurés dans l'Administrateur des services Windows Media pour prendre en charge ces scénarios de diffusion HTTP supplémentaires.

À propos de la substitution de protocole

Si les clients qui prennent en charge RTSP se connectent à un serveur qui exécute les services Windows Media® avec un nom d'URL RTSP (par exemple, rtsp://) ou un nom d'URL MMS (par exemple, mms://), le serveur utilise le transfert de protocole pour diffuser le contenu au client afin de fournir une expérience de diffusion optimale. Le transfert automatique de protocole entre RTSP/MMS et RTSP avec des transports basés sur UDP ou TCP (RTSPU ou RTSPT), ou même HTTP (si le plug-in WMS HTTP Server Control Protocol est activé) peut se produire lorsque le serveur tente de négocier le meilleur protocole et de fournir une expérience de diffusion optimale pour le client. Les clients qui prennent en charge RTSP incluent Windows Media Player 9 ou version ultérieure ou d'autres lecteurs qui utilisent le contrôle ActiveX de Windows Media Player 9.

Les versions antérieures du Lecteur Windows Media, telles que le Lecteur Windows Media pour Windows XP, ne prennent pas en charge le protocole RTSP, mais le protocole MMS assure la prise en charge du transfert de protocole pour ces clients. Ainsi, lorsqu'une version antérieure du Lecteur tente de se connecter au serveur avec un moniker d'URL MMS, le transfert automatique de protocole de MMS à MMS avec des transports basés sur UDP ou TCP (MMSU ou MMST), ou même HTTP (si le plug-in WMS HTTP Server Control Protocol est activé), peut se produire lorsque le serveur tente de négocier le meilleur protocole et de fournir une expérience de diffusion optimale pour ces clients.

Afin de s'assurer que votre contenu est disponible pour tous les clients qui se connectent à votre serveur, les ports de votre pare-feu doivent être ouverts pour tous les protocoles de connexion qui peuvent être utilisés dans le cadre du transfert de protocole.

Vous pouvez forcer votre serveur Windows Media à 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 de diffusion optimale pour toutes les versions client, nous recommandons que l'URL utilise le protocole MMS général. Si les clients se connectent à votre flux avec une URL avec un moniker d'URL MMS, tout transfert de protocole nécessaire se produit automatiquement. Notez que les utilisateurs peuvent désactiver les protocoles de diffusion en continu dans les paramètres de propriété du Lecteur Windows Media. Si un utilisateur désactive un protocole, il est ignoré lors de la substitution. Par exemple, si HTTP est désactivé, les URL ne sont pas transférées vers HTTP.

Affecter des ports aux services Windows Media

La plupart des pare-feu sont utilisés pour contrôler le « trafic entrant » vers le serveur ; ils ne contrôlent généralement pas le « trafic sortant » vers les clients. Les ports de votre pare-feu pour le trafic sortant peuvent être fermés si une stratégie de sécurité plus stricte est mise en oeuvre sur votre réseau de serveurs. Cette section décrit l'allocation de port par défaut pour Windows Media® Services pour le trafic entrant et sortant (indiqué dans les tableaux comme « Entrant » et « Sortant ») afin que vous puissiez configurer tous les ports selon les besoins.

Dans certains scénarios, le trafic sortant peut être dirigé vers un port dans une plage de ports disponibles. Les plages de ports indiquées dans les tableaux indiquent la plage complète des ports disponibles, mais vous pouvez allouer moins de ports dans la plage de ports. Lorsque vous décidez du nombre de ports à ouvrir, équilibrez la sécurité avec l'accessibilité et ouvrez juste assez de ports pour permettre à tous les clients d'établir une connexion. Tout d'abord, déterminez le nombre de ports que vous prévoyez utiliser pour Windows Media Services, puis ouvrez 10 % de plus pour tenir compte du chevauchement avec d'autres programmes. Après avoir établi ce numéro, surveillez votre trafic pour déterminer si des ajustements sont nécessaires.

Les restrictions de plage de ports peuvent affecter toutes les applications RPC (Remote Procedure Call) et DCOM (Distributed Component Object Model) qui partagent le système, et pas seulement les services Windows Media. Si la plage de ports allouée n'est pas assez large, les services concurrents tels que IIS peuvent échouer avec des erreurs aléatoires. La plage de ports doit être capable de prendre en charge toutes les applications système potentielles qui utilisent des services RPC, COM ou DCOM.

Afin de faciliter la configuration du pare-feu, vous pouvez configurer chaque plug-in de protocole de contrôle de serveur (RTSP, MMS et HTTP) dans l'administrateur des services Windows Media pour utiliser un port spécifique. Si votre administrateur réseau a déjà ouvert une série de ports à utiliser par votre serveur Windows Media, vous pouvez allouer ces ports aux protocoles de contrôle en conséquence. Si ce n'est pas le cas, vous pouvez demander à l'administrateur réseau d'ouvrir les ports par défaut de chaque protocole. S'il n'est pas possible d'ouvrir des ports sur votre pare-feu, Windows Media Services peut diffuser du contenu avec le protocole HTTP sur le port 80.

Il s'agit de l'allocation de port de pare-feu par défaut pour Windows Media Services afin de fournir un flux de monodiffusion :

Protocole d'application	Protocol	Port	Description
RTSP	TCP	554 (entrée/sortie)	Utilisé pour accepter les connexions entrantes des clients RTSP et pour transmettre des paquets de données aux clients qui diffusent avec RTSPT.
RTSP	UDP	5004 (sortie)	Utilisé pour transmettre des paquets de données aux clients qui diffusent avec RTSPU.
RTSP	UDP	5005 (entrée/sortie)	Utilisé pour recevoir des informations de perte de paquets de clients et fournir des informations de synchronisation

			aux clients qui diffusent avec RTSPU.
MMS	TCP	1755 (entrée/sortie)	Utilisé pour accepter les connexions de client MMS entrantes et pour transmettre des paquets de données aux clients qui diffusent avec MMST.
MMS	UDP	1755 (entrée/sortie)	Utilisé pour recevoir des informations de perte de paquets de clients et fournir des informations de synchronisation aux clients qui diffusent avec MMSU.
MMS	UDP	1024-5000 (sortie)	Utilisé pour transmettre des paquets de données aux clients qui diffusent en continu avec MMSU. Ouvrez uniquement le nombre de ports nécessaire.
HTTP	TCP	80 (entrée/sortie)	Utilisé pour accepter les connexions de clients HTTP entrants et pour transmettre des paquets de données aux clients qui diffusent avec HTTP.

Afin de vous assurer que votre contenu est disponible pour toutes les versions clientes qui se connectent à votre serveur, ouvrez tous les ports décrits dans le tableau pour tous les protocoles de connexion qui peuvent être utilisés dans le cadre du transfert de protocole. Si vous exécutez Windows Media Services sur un ordinateur qui exécute Windows Server™ 2003 Service Pack 1 (SP1), vous devez ajouter le programme Windows Media Services (wmserver.exe) en tant qu'exception dans le Pare-feu Windows pour ouvrir les ports entrants par défaut pour la diffusion monodiffusion, plutôt que d'ouvrir manuellement les ports dans le pare-feu.

Remarque : Reportez-vous au site Web de Microsoft pour en savoir plus sur la configuration du pare-feu MMS.

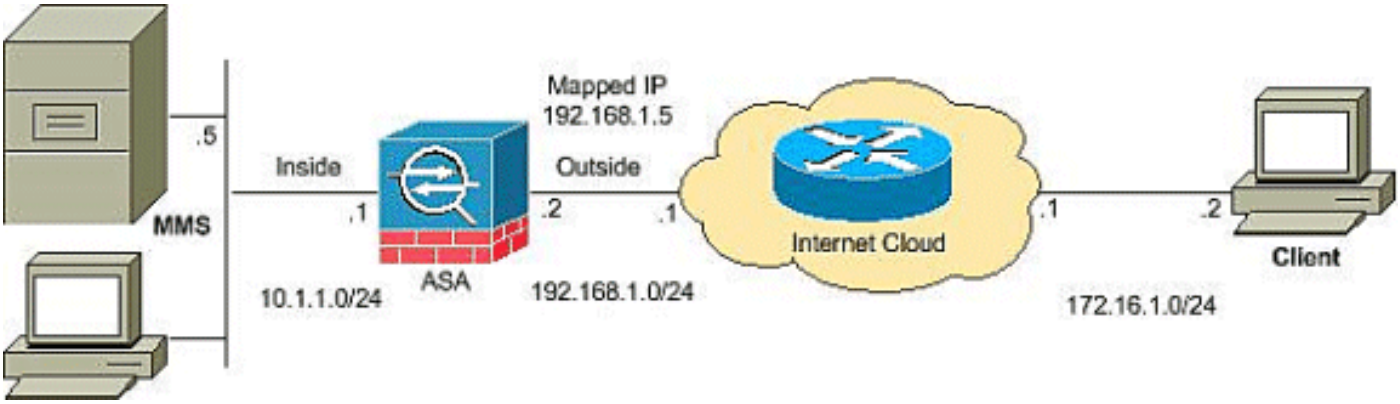
Configuration

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

Remarque : utilisez l'outil de recherche de commandes (clients enregistrés uniquement) 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 IP utilisés dans cette configuration ne sont pas routables légalement 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
```

Vérification

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 .**

- **Show access-list** — Affiche les listes de contrôle d'accès configurées dans 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
```

- **Show nat** : affiche les stratégies et les compteurs NAT.

```
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
```

Difficultés liées à la diffusion vidéoDépannage

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

Inspecter RTSP est une configuration par défaut sur l'ASA. Il casse le trafic MMS car l'appliance de sécurité ne peut pas effectuer la NAT sur les messages RTSP, car les adresses IP intégrées sont contenues dans les fichiers SDP dans le cadre de messages HTTP ou RTSP. Les paquets peuvent être fragmentés et le dispositif de sécurité ne peut pas effectuer la NAT sur les paquets fragmentés.

Solution de contournement: Ce problème peut être résolu si vous désactivez l'inspection RTSP pour ce trafic MMS particulier, comme indiqué :

```
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 d'assistance Cisco ASA
- Support et documentation techniques - Cisco Systems