ASA/PIX: Laat het netwerkverkeer toegang hebben tot de Microsoft Media Server (MMS) / streaming video in het configuratievoorbeeld van Internet

Inhoud

Inleiding

Dit document beschrijft hoe de adaptieve security applicatie (ASA) moet worden configureren, zodat de client of gebruiker vanaf het internet toegang kan krijgen tot de Microsoft Media Server (MMS) of streaming video die in het netwerk van ASA is geplaatst.

Voorwaarden

Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- Basisconfiguratie van ASA
- MMS is ingesteld en werkt goed

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco ASA dat softwareversie 7.x en hoger uitvoert.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Verwante producten

De informatie in dit document is ook van toepassing op Cisco PIX Firewall die softwareversie 7.x en hoger uitvoert.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Firewallinformatie voor Windows Media Services 9 Series

Streamingmediaprotocollen gebruiken

Microsoft® Windows Media® Services 9 Series gebruikt twee streaming media protocols om content als een unicast stream aan klanten te leveren:

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

Deze protocollen ondersteunen client-controle acties zoals stop, pauze, terugspoelen en snel-voorwaartse geïndexeerde Windows-mediabestanden.

RTSP is een toepassingslaag protocol dat specifiek werd gemaakt om gecontroleerde levering van real-time gegevens, zoals audio en video inhoud te voorzien. U kunt RTSP gebruiken om inhoud te stroomen naar computers die Windows Media Player 9 Series of hoger uitvoeren, naar klanten die de actieveX®-controle van Windows Media Player 9 Series gebruiken of naar andere computers die Windows Media Services 9 Series uitvoeren. RTSP werkt in combinatie met Real-Time Transport Protocol (RTP) om pakketten multimedia-inhoud te formatteren en het meest efficiënte transport-laagprotocol te onderhandelen, of User Datagram Protocol (UDP) of Transport Control Protocol (TCP), om te gebruiken wanneer u de stroom aan klanten levert. U kunt RTSP implementeren via de WMS RTSP Server Control Protocol-plug-in in Windows Media Services beheerder. Deze instekker is standaard ingeschakeld.

MMS is een eigen toepassingslaag protocol dat is ontwikkeld voor eerdere versies van Windows Media Services. U kunt MMS gebruiken om inhoud te stroomlijnen naar computers die Windows Media Player voor Windows® XP of hoger uitvoeren. U kunt MMS implementeren via de plug-in van WMS Server Control Protocol in Windows Media Services beheerder. Deze instekker is standaard ingeschakeld.

HTTP gebruiken

Als poorten op uw firewall niet kunnen worden geopend, kunnen Windows Media® Services inhoud met HTTP over poort 80 stroomlijnen. HTTP kan worden gebruikt om stromen naar alle versies van Windows Media Player te leveren. U kunt HTTP implementeren via de WMS HTTP Server Control Protocol-plug-in in Windows Media Services beheerder. Deze instekker is standaard niet ingeschakeld. Als een andere service, zoals Internet Information Services (IS), poort 80 op hetzelfde IP-adres gebruikt, kunt u de plug-in niet inschakelen.

HTTP kan ook worden gebruikt voor:

- Gedistribueerde stromen tussen Windows Media-servers
- Broninhoud van een Windows-media-encoder
- Downloadt dynamisch gegenereerde afspeellijsten van een webserver

Plug-ins voor gegevensbronnen moeten in Windows Media Services beheerder worden geconfigureerd om deze extra HTTP-streaming scenario's te ondersteunen.

Over Protocol-omloop

Als klanten die RTSP ondersteunen verbinding maken met een server die Windows Media® Services runt met een RTSP URL moniker (bijvoorbeeld rtsp://) of een MMS URL moniker (bijvoorbeeld mms://), gebruikt de server protocol rollover om de inhoud naar de client te stroomlijnen om een optimale streaming ervaring te leveren. Automatische protocolomzetting van RTSP/MMS naar RTSP met op UDP gebaseerde of op TCP gebaseerde transport (RTSPU of RTSPT), of zelfs HTTP (als de plug-in van het HTTP Server Control Protocol van WMS is ingeschakeld) kan voorkomen als de server probeert te onderhandelen over het beste protocol en een optimale streamingervaring voor de client biedt. Clients die RTSP ondersteunen, zijn Windows Media Player 9 Series of hoger of andere spelers die de Windows Media Player 9 Series ActiveX-controller gebruiken.

Eerdere versies van Windows Media Player, zoals Windows Media Player for Windows XP, ondersteunen het RTSP-protocol niet, maar het MMS-protocol biedt ondersteuning voor protocolrollover voor deze klanten. Wanneer een eerdere versie van de Player probeert om verbinding te maken met de server met een MMS URL-moniker, kan automatisch protocol omversen van MMS naar MMS met op UDP gebaseerde of TCP-gebaseerde transport (MMSU of MMST) of zelfs HTTP (als de plug-in van WMS HTTP Server Control Protocol is ingeschakeld) plaatsvinden als de server probeert het beste protocol te onderhandelen en een optimale streaming ervaring voor deze clients levert.

Om ervoor te zorgen dat uw inhoud beschikbaar is voor alle klanten die aan uw server verbinden, moeten de poorten op uw firewall worden geopend voor alle verbindingsprotocollen die kunnen worden gebruikt binnen het protocol rollover.

U kunt uw Windows Media server dwingen om een specifiek protocol te gebruiken als u het protocol identificeert dat in het aankondigingsbestand gebruikt moet worden (bijvoorbeeld rtspu://server/publishing_point/file). Om een optimale streaming ervaring voor alle clientversies te bieden, raden we aan dat de URL het algemene MMS-protocol gebruikt. Als klanten met een URL met een MMS URL moniker aan uw stroom verbinden, komt elke noodzakelijke protocol rollover automatisch voor. Houd in acht dat gebruikers streamingprotocollen kunnen uitschakelen in de instellingen voor Windows Media Player. Als een gebruiker een protocol uitschakelt, wordt het overgeslagen. Bijvoorbeeld, als HTTP wordt gehandicapt, rollen de URLs niet over naar HTTP.

Ports voor Windows-mediaservices toewijzen

De meeste firewalls worden gebruikt om "inkomend verkeer" naar de server te controleren; over het algemeen beheersen zij het " uitgaande verkeer " naar klanten niet . De poorten in uw firewall voor uitgaande verkeer kunnen worden gesloten als een strenger veiligheidsbeleid op uw servernetwerk wordt uitgevoerd. In dit gedeelte wordt de standaardpoortindeling voor Windows Media® Services beschreven voor zowel inkomende als uitgaande verkeer (weergegeven als "In" en "Out" in de tabellen) zodat u alle poorten naar wens kunt configureren.

In sommige scenario's kan het uitgaande verkeer naar één poort worden gericht in een reeks beschikbare poorten. Poortbereik in de tabellen geeft het gehele bereik van de beschikbare poorten aan, maar u kunt minder poorten binnen het poortbereik toewijzen. Wanneer u besluit hoeveel poorten te openen zijn, moet u de beveiliging in evenwicht brengen met toegankelijkheid en net genoeg poorten openen om alle klanten in staat te stellen een verbinding te maken. Bepaal eerst hoeveel poorten je verwacht te gebruiken voor Windows Media Services en open dan 10 procent meer om rekening te houden met overlap met andere programma's. Nadat u dit nummer hebt ingesteld, controleert u of er aanpassingen nodig zijn.

Poortbeperkingen hebben mogelijk invloed op alle toepassingen van de afstandsbediening (RPC) en het Gedistribueerde Component Object Model (DCOM) die het systeem delen, en niet alleen op Windows Media Services. Als het toegewezen havenbereik niet breed genoeg is, kunnen de concurrerende diensten zoals IS met willekeurige fouten mislukken. Het poortbereik moet geschikt zijn voor alle potentiële systeemtoepassingen die gebruik maken van de diensten van RPC, COM of DCOM.

Om de configuratie van firewalls eenvoudiger te maken, kunt u elk protocol-plug-in (RTSP, MMS en HTTP) van de servercontrole configureren in een specifieke poort. Als uw netwerkbeheerder al een reeks poorten voor gebruik door uw Windows Media server heeft geopend, kunt u deze poorten aan de besturingsprotocollen toewijzen. Als dit niet het geval is, kunt u de netwerkbeheerder vragen om de standaardpoorten voor elk protocol te openen. Als het niet mogelijk is om poorten op uw firewall te openen, kunnen Windows Media Services inhoud met het HTTP-protocol stream over poort 80.

Dit is de standaard firewallpoorttoewijzing voor Windows Media Services om een eenaststroom te leveren:

Toepassingsprotocol	Protocol	Port	Beschrijving
RTSP	TCP	554 (in/uit)	Gebruikt om inkomende RTSP clientverbindingen te accepteren en om datapakketten aan klanten te leveren die met RTSPT streamen.
RTSP	UDP	5004 (uit)	Gebruikt om gegevenspakketten aan cliënten te leveren die met RTSPU stromen.
RTSP	UDP	5005 (in/uit)	Gebruikt om pakketverlies informatie van cliënten te ontvangen en synchronisatieinformatie te verstrekken aan cliënten die met RTSPU stromen.
MMS	TC	1755	Gebruikt om inkomende MMS

	P	(in/uit)	clientverbindingen te accepteren en gegevenspakketten te leveren aan klanten die streamen met MMST.
MMS	UDP	1755 (in/uit)	Gebruikt om pakketverliesinformatie van klanten te ontvangen en synchronisatie-informatie te verstrekken aan klanten die met MMSU stromen.
MMS	UDP	1024 - 5000 (uit)	Gebruikt om gegevenspakketten aan klanten te leveren die met MMSU streamen. Open alleen het gewenste aantal poorten.
HTTP	TCP	80 (in/uit)	Gebruikt om inkomende HTTP clientverbindingen te accepteren en gegevenspakketten aan klanten te leveren die streaming zijn met HTTP.

Om ervoor te zorgen dat uw inhoud beschikbaar is voor alle clientversies die op uw server aansluiten, opent u alle poorten die in de tabel zijn beschreven voor alle verbindingsprotocollen die kunnen worden gebruikt binnen het protocol rollover. Als u Windows Media Services op een computer runt die Windows Server™ 2003 Service Pack 1 (SP1) draait, moet u het Windows Media Services-programma (wmserver.exe) als uitzondering in Windows Firewall toevoegen om de standaard inkomende poorten voor unicast streaming te openen in plaats van poorten handmatig in de firewall.

Opmerking: Raadpleeg de Microsoft website voor meer informatie over de MMS-firewallconfiguratie.

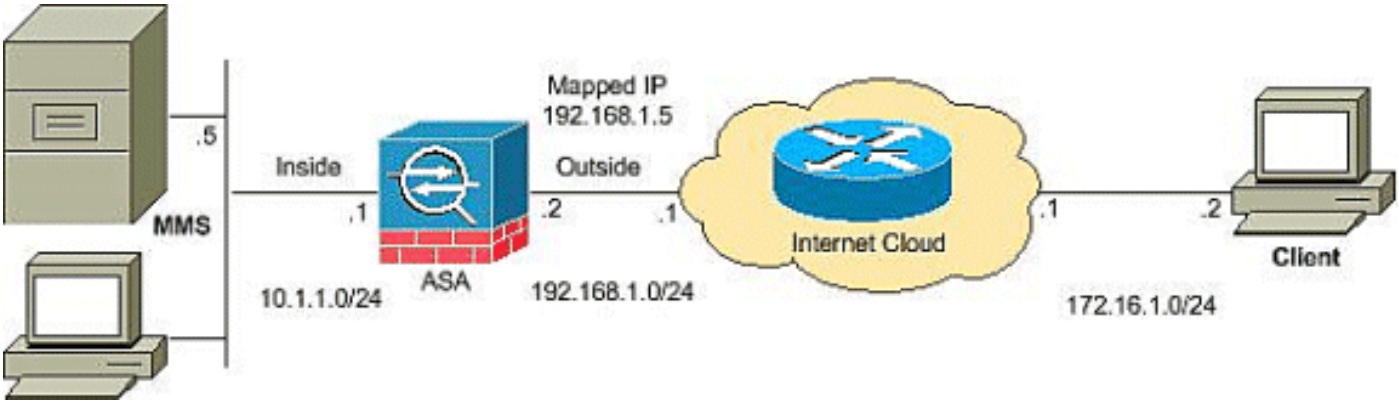
Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het Opname Gereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Opmerking: de IP-adresseringsschema's die in deze configuratie worden gebruikt, zijn niet wettelijk routeerbaar op het internet. Ze zijn RFC 1918-adressen die in een labomgeving zijn gebruikt.

Configuraties

Dit document gebruikt deze configuraties:

ASA-configuratie

```
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
```

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

- **Toegangslijst tonen** — Hiermee worden de ACL's weergegeven die in de ASA/PIX zijn geconfigureerd

```
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
```

- **NAT**-displays NAT beleid en tellers tonen

```
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
```

Video-probleemoplossing streamen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Controleer RTSP is een standaardconfiguratie voor de ASA. Het breekt het MMS-verkeer omdat het security apparaat geen NAT kan uitvoeren op RTSP-berichten omdat de ingesloten IP-adressen in de SDP-bestanden zitten als onderdeel van HTTP- of RTSP-berichten. Packets kunnen gefragmenteerd zijn en het security apparaat kan geen NAT op gefragmenteerde pakketten uitvoeren.

Werken: Dit probleem kan worden opgelost als u de RTSP-inspectie voor dit specifieke MMS-verkeer zoals wordt weergegeven uitschakelt:

```
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
```

Gerelateerde informatie

- Cisco PIX-firewallsoftware
- Opdrachtreferenties van Cisco Secure PIX-firewall
- Security meldingen uit het veld (inclusief PIX)
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning - Cisco-systemen
- Cisco ASA-ondersteuningspagina
- Technische ondersteuning en documentatie – Cisco Systems