ASA/PIX:네트워크 트래픽이 인터넷 컨피그레이션 예시에서 Microsoft Media Server(MMS)/스트리밍 비디오에 액세스하도록 허용

목차

소개

이 문서에서는 인터넷에서 클라이언트 또는 사용자가 ASA의 내부 네트워크에 배치된 Microsoft Media Server(MMS) 또는 스트리밍 비디오에 액세스할 수 있도록 하기 위해 ASA(Adaptive Security Appliance)를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- ASA의 기본 구성
- MMS가 구성되고 제대로 작동합니다.

사용되는 구성 요소

이 문서의 정보는 소프트웨어 버전 7.x 이상을 실행하는 Cisco ASA를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

관련 제품

이 문서의 정보는 소프트웨어 버전 7.x 이상을 실행하는 Cisco PIX 방화벽에도 적용됩니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

Windows Media Services 9 Series용 방화벽 정보

스트리밍 미디어 프로토콜 사용

Microsoft® Windows Media® Services 9 Series는 2개의 스트리밍 미디어 프로토콜을 사용하여 클라이언트에 콘텐츠를 유니캐스트 스트림으로 전달합니다.

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

이러한 프로토콜은 인덱싱된 Windows Media 파일 중지, 일시 중지, 되감기 및 빠른 전달 등의 클라이언트 제어 작업을 지원합니다.

RTSP는 오디오 및 비디오 콘텐츠와 같은 실시간 데이터의 제어된 전달을 제공하기 위해 특별히 만들어진 애플리케이션 레이어 프로토콜입니다.RTSP를 사용하여 Windows Media Player 9 Series 이상을 실행하는 컴퓨터, Windows Media Player 9 Series ActiveX® 컨트롤을 사용하는 클라이언트 또는 Windows Media Services 9 Series를 실행하는 다른 컴퓨터로 콘텐츠를 스트리밍할 수 있습니다.RTSP는 RTP(Real-Time Transport Protocol)와 함께 작동하여 멀티미디어 콘텐츠의 패킷을 포맷하고 가장 효율적인 전송 계층 프로토콜(UDP(User Datagram Protocol) 또는 TCP(Transport Control Protocol)를 협상하여 스트림을 클라이언트에 전달할 때 사용합니다.Windows Media 서비스 관리자의 WMS RTSP 서버 제어 프로토콜 플러그인을 통해 RTSP를 구현할 수 있습니다.이 플러그인은 기본적으로 활성화되어 있습니다.

MMS는 이전 버전의 Windows Media Services용으로 개발된 전용 애플리케이션 레이어 프로토콜입니다.MMS를 사용하여 Windows® XP 이전 버전의 Windows Media Player를 실행하는 컴퓨터로 콘텐츠를 스트리밍할 수 있습니다.Windows Media 서비스 관리자의 WMS MMS 서버 제어 프로토콜 플러그인을 통해 MMS를 구현할 수 있습니다.이 플러그인은 기본적으로 활성화되어 있습니다.

HTTP 사용

방화벽의 포트를 열 수 없는 경우 Windows Media® Services는 포트 80을 통해 HTTP로 콘텐츠를 스트리밍할 수 있습니다. HTTP를 사용하여 모든 Windows Media Player 버전에 스트림을 전달할 수 있습니다.Windows Media 서비스 관리자의 WMS HTTP 서버 제어 프로토콜 플러그인을 통해 HTTP를 구현할 수 있습니다.이 플러그인은 기본적으로 활성화되어 있지 않습니다.IIS(인터넷 정보 서비스)와 같은 다른 서비스에서 동일한 IP 주소에서 포트 80을 사용하는 경우 플러그인을 활성화할 수 없습니다.

HTTP는 다음 항목에도 사용할 수 있습니다.

- Windows Media 서버 간에 스트림 배포
- Windows Media 인코더의 소스 콘텐츠
- 웹 서버에서 동적으로 생성된 재생 목록 다운로드

이러한 추가 HTTP 스트리밍 시나리오를 지원하려면 Windows Media 서비스 관리자에서 데이터 소스 플러그인을 구성해야 합니다.

프로토콜 롤오버 정보

RTSP를 지원하는 클라이언트가 RTSP URL 모니커(예: rtsp://) 또는 MMS URL 모니커(예: mms://)을 사용하여 Windows Media® Services를 실행하는 서버에 연결되면 서버는 프로토콜 롤오버레이를 사용하여 클라이언트에 콘텐츠를 스트리밍하여 최적의 스트리밍 환경을 제공합니다 .UDP 기반 또는 TCP 기반 전송(RTSPU 또는 RTSPT) 또는 HTTP(WMS HTTP Server Control Protocol 플러그인이 활성화된 경우)를 사용하는 경우 RTSP/MMS에서 RTSP로 자동 프로토콜 롤오버가 발생할 수 있으며, 서버가 최상의 프로토콜을 협상하고 클라이언트에 최적의 스트리밍 환경을 제공합니다.RTSP를 지원하는 클라이언트에는 Windows Media Player 9 Series 이상 또는 Windows Media Player 9 Series ActiveX 컨트롤을 사용하는 다른 플레이어가 포함됩니다.

Windows XP용 Windows Media Player와 같은 이전 버전의 Windows Media Player는 RTSP 프로토콜을 지원하지 않지만 MMS 프로토콜은 이러한 클라이언트에 대한 프로토콜 롤오버 지원을 제공합니다.따라서 이전 버전의 Windows Media Player가 MMS URL 모니커를 사용하여 서버에 연결하려고 할 때, UDP 기반 또는 TCP 기반 전송(MMSU 또는 MMST) 또는 심지어 HTTP(WMS HTTP Server Control Protocol 플러그인이 활성화된 경우)를 통해 MMS에서 MMS로 자동 프로토콜 롤오버가 발생하거나 서버가 최상의 프로토콜을 협상하고 이러한 클라이언트에 최적의 스트리밍 환경을 제공할 수 있습니다.

서버에 연결하는 모든 클라이언트에서 콘텐츠를 사용할 수 있도록 하려면 프로토콜 롤오버 내에서 사용할 수 있는 모든 연결 프로토콜에 대해 방화벽의 포트를 열어야 합니다.

알림 파일에서 사용할 프로토콜을 식별하면 Windows Media 서버에서 특정 프로토콜을 사용하도록 강제할 수 있습니다(예: rtspu://server/publishing_point/file). 모든 클라이언트 버전에 최적의 스트리밍 환경을 제공하려면 URL에서 일반 MMS 프로토콜을 사용하는 것이 좋습니다.클라이언트가 MMS URL 모니커가 있는 URL을 사용하여 스트림에 연결하는 경우 필요한 모든 프로토콜 롤오버가 자동으로 발생합니다.사용자는 Windows Media Player 속성 설정에서 스트리밍 프로토콜을 비활성화할 수 있습니다.사용자가 프로토콜을 비활성화하면 롤오버 내에서 건너뜁니다.예를 들어 HTTP가 비활성화된 경우 URL은 HTTP로 롤오버되지 않습니다.

Windows Media 서비스에 포트 할당

대부분의 방화벽은 서버에 대한 "인바운드 트래픽"을 제어하는 데 사용됩니다.일반적으로 클라이언트에 대한 "아웃바운드 트래픽"을 제어하지 않습니다.서버 네트워크에 더 엄격한 보안 정책이 구현되면 방화벽의 아웃바운드 트래픽용 포트를 닫을 수 있습니다.이 섹션에서는 필요에 따라 모든 포트를 구성할 수 있도록 인바운드 및 아웃바운드 트래픽 모두에 대한 Windows Media® 서비스의 기본 포트 할당(테이블의 "수신" 및 "발신"으로 표시됨)에 대해 설명합니다.

일부 시나리오에서는 사용 가능한 포트 범위에 있는 하나의 포트로 아웃바운드 트래픽을 전달할 수 있습니다.테이블에 표시된 포트 범위는 사용 가능한 포트의 전체 범위를 나타내지만 포트 범위 내에서 더 적은 수의 포트를 할당할 수 있습니다.열 포트 수를 결정할 때 보안과 액세스 가능성 간의 균형을 맞추고 모든 클라이언트가 연결할 수 있도록 충분한 포트만 엽니다.먼저 Windows Media 서비스에 사용할 포트 수를 결정한 다음 다른 프로그램과 겹치기 위해 10% 더 열어 보십시오.이 번호

를 설정한 후 트래픽을 모니터링하여 조정이 필요한지 확인합니다.

포트 범위 제한은 Windows Media 서비스뿐만 아니라 시스템을 공유하는 모든 RPC(원격 프로시저 호출) 및 DCOM(분산 구성 요소 개체 모델) 응용 프로그램에 영향을 줄 수 있습니다.할당된 포트 범위가 충분히 넓지 않으면 IIS와 같은 경쟁 서비스가 랜덤 오류로 인해 실패할 수 있습니다.포트 범위는 RPC, COM 또는 DCOM 서비스를 사용하는 모든 잠재적 시스템 응용 프로그램을 수용할 수 있어야 합니다.

방화벽 구성을 쉽게 하기 위해 Windows Media 서비스 관리자에서 특정 포트를 사용하도록 각 서버 제어 프로토콜 플러그인(RTSP, MMS 및 HTTP)을 구성할 수 있습니다.네트워크 관리자가 Windows Media 서버에서 사용할 수 있도록 일련의 포트를 이미 연 경우 해당 포트를 제어 프로토콜에 적절하게 할당할 수 있습니다.그렇지 않은 경우 네트워크 관리자에게 각 프로토콜에 대한 기본 포트를 열도록 요청할 수 있습니다.방화벽에서 포트를 열 수 없는 경우 Windows Media 서비스는 포트 80을 통해 HTTP 프로토콜을 사용하여 콘텐츠를 스트리밍할 수 있습니다.

유니캐스트 스트림을 전달하기 위한 Windows Media Services의 기본 방화벽 포트 할당입니다.

애플리케이션 프로토콜	프로토콜	포트	설명
RTSP	TCP	554(수신/발신)	인바운드 RTSP 클라이언트 연결을 수락하고 RTSPT를 사용하여 스트리밍하는 클라이언트에 데이터 패킷을 전달하는 데 사용됩니다.
RTSP	UDP	5004(발신)	RTSPU로 스트리밍되는 클라이언트에 데이터 패킷을 전달하는 데 사용됩니다.
RTSP	UDP	5005(수신/발신)	클라이언트에서 패킷 손실 정보를 수신하고 RTSPU를 사용하여 스트리밍하는 클라이언트에 동기화 정보를 제공하는 데 사용됩니다.
MMS	TCP	1755(수신/발신)	인바운드 MMS 클라이언트 연결을 수락하고 MMST를 사용하여 스트리밍하는 클라이언트에 데이터 패킷을 전달하는 데 사용됩니다.
MMS	UDP	1755(수신/발신)	클라이언트에서 패킷 손실 정보를 수신하고 MMSU를 사용하여 스트리밍하는 클라이언트에 동기화 정보를 제공하는 데 사용됩니다.
MMS	UDP	1024-5000(발신)	MMSU를 사용하여 스트리밍하는 클라이언트에 데이터 패킷을 전달하는 데 사용됩니다.필요한 포트 수만 엽니다.
HTTP	TCP	80(수신/발신)	인바운드 HTTP 클라이언트 연결을 수락하고 HTTP를 사용하여 스트리밍하는 클라이언트에 데이터 패킷을 전달하는 데 사용됩니다.

서버에 연결하는 모든 클라이언트 버전에서 콘텐츠를 사용할 수 있도록 하려면 프로토콜 롤오버 내에서 사용할 수 있는 모든 연결 프로토콜에 대해 표에 설명된 모든 포트를 엽니다.Windows Server™ 2003 서비스 팩 1(SP1)을 실행하는 컴퓨터에서 Windows Media 서비스를 실행하는 경우 방화벽에서 포트를 수동으로 열지 않고 유니캐스트 스트리밍을 위한 기본 인바운드 포트를 열려면 Windows 방화벽에서 Windows Media 서비스 프로그램(wmserver.exe)을 예외로 추가해야 합니다.

참고: MMS 방화벽 컨피그레이션에 대한 자세한 내용은 Microsoft 웹 사이트 를 참조하십시오.

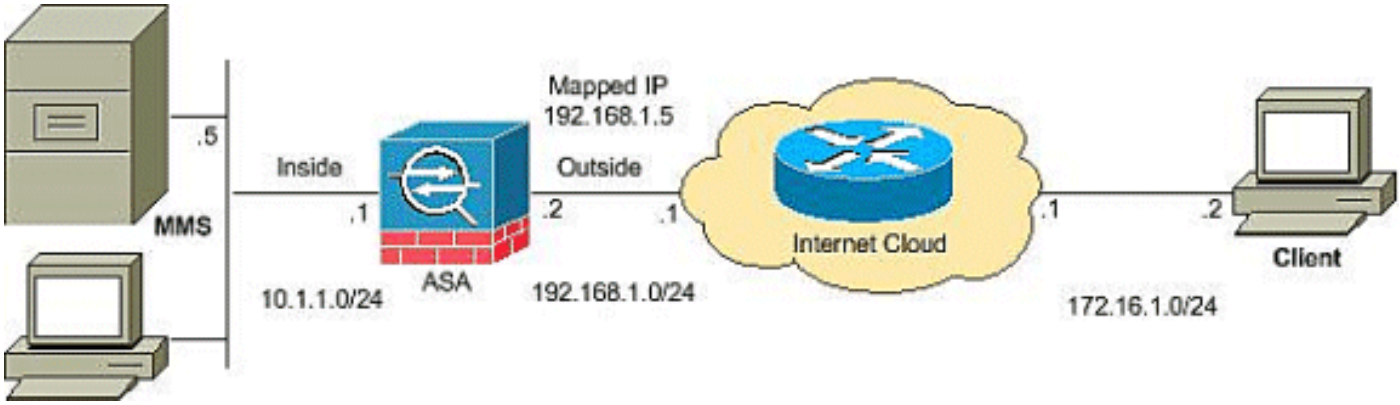
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



참고: 이 구성에 사용된 IP 주소 지정 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다.실습 환경에서 사용된 RFC 1918 주소입니다.

구성

이 문서에서는 다음 구성을 사용합니다.

ASA 컨피그레이션

```
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
```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

- **Show access-list** — ASA/PIX에 구성된 ACL을 표시합니다.

```
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** - NAT 정책 및 카운터를 표시합니다.

```
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
```

스트리밍 비디오문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

Inspect RTSP는 ASA의 기본 컨피그레이션입니다.포함된 IP 주소가 HTTP 또는 RTSP 메시지의 일부로 SDP 파일에 포함되므로 보안 어플라이언스에서 RTSP 메시지에 대해 NAT를 수행할 수 없으므로 MMS 트래픽이 중단됩니다.패킷은 프래그먼트화될 수 있으며, 보안 어플라이언스는 프래그먼트된 패킷에 대해 NAT를 수행할 수 없습니다.

해결 방법:다음과 같이 이 특정 MMS 트래픽에 대해 RTSP 검사를 비활성화하면 이 문제를 해결할 수 있습니다.

```
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
```

관련 정보

- Cisco PIX 방화벽 소프트웨어
- Cisco Secure PIX Firewall 명령 참조
- 보안 제품 필드 알림(PIX 포함)
- RFC(Request for Comments)
- Technical Support - Cisco Systems
- Cisco ASA 지원 페이지
- 기술 지원 및 문서 – Cisco Systems