ASA/PIX: Ermöglichen Sie dem Netzwerkverkehr den Zugriff auf den Microsoft Media Server (MMS)/Streaming Video aus dem Konfigurationsbeispiel Internet.

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die Adaptive Security Appliance (ASA) so konfiguriert wird, dass der Client oder der Benutzer aus dem Internet auf den Microsoft Media Server (MMS) oder das Streaming-Video im internen Netzwerk der ASA zugreifen kann.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Basiskonfiguration der ASA
- MMS ist konfiguriert und funktioniert ordnungsgemäß

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco ASA, die Software Version 7.x und höher ausführt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Zugehörige Produkte

Die Informationen in diesem Dokument gelten auch für die Cisco PIX-Firewall, auf der die Software Version 7.x und höher ausgeführt wird.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Firewall-Informationen für Windows Media Services der Serie 9

Streaming-Media-Protokolle verwenden

Die Microsoft® Windows Media® Services 9-Serie verwendet zwei Streaming-Medienprotokolle, um den Clients Inhalte als Unicast-Stream bereitzustellen:

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

Diese Protokolle unterstützen Clientsteueraktionen wie Stoppen, Anhalten, Zurückspulen und schnelle Weiterleitung indizierter Windows Media-Dateien.

RTSP ist ein Protokoll auf Anwendungsebene, das speziell für die kontrollierte Bereitstellung von Echtzeitdaten wie Audio- und Videoinhalten entwickelt wurde. Sie können RTSP verwenden, um Inhalte an Computer zu streamen, auf denen Windows Media Player 9 Series oder höher ausgeführt wird, an Clients, die das ActiveX®-Steuerelement der Windows Media Player 9 Series verwenden, oder an andere Computer, auf denen die Windows Media Services 9 Series ausgeführt wird. RTSP arbeitet mit Real-Time Transport Protocol (RTP) zusammen, um Pakete mit Multimedia-Inhalten zu formatieren und das effizienteste Transportschichtprotokoll auszuhandeln, entweder User Datagram Protocol (UDP) oder Transport Control Protocol (TCP), das beim Übertragen des Streams an Clients verwendet wird. Sie können RTSP über das WMS RTSP Server Control Protocol-Plug-in in Windows Media Services Administrator implementieren. Dieses Plug-in ist standardmäßig aktiviert.

MMS ist ein proprietäres Anwendungs-Layer-Protokoll, das für frühere Versionen von Windows Media Services entwickelt wurde. Sie können MMS verwenden, um Inhalte auf Computern zu streamen, auf denen Windows Media Player für Windows® XP oder früher ausgeführt wird. Sie können MMS über das WMS MMS Server Control Protocol-Plug-in in Windows Media Services Administrator implementieren. Dieses Plug-in ist standardmäßig aktiviert.

HTTP verwenden

Wenn Ports auf Ihrer Firewall nicht geöffnet werden können, können Windows Media® Services Inhalte mit HTTP über Port 80 streamen. HTTP kann verwendet werden, um Streams an alle Windows Media Player-Versionen zu senden. Sie können HTTP über das WMS HTTP Server Control Protocol-Plug-in in Windows Media Services Administrator implementieren. Dieses Plug-in ist nicht standardmäßig aktiviert. Wenn ein anderer Dienst, z. B. Internetinformationsdienste (IIS), Port 80 auf derselben IP-Adresse verwendet, können Sie das Plug-in nicht aktivieren.

HTTP kann auch für folgende Zwecke verwendet werden:

- Streams zwischen Windows Media-Servern verteilen
- Quellinhalte aus einem Windows Media Encoder
- Dynamisch generierte Playlists von einem Webserver herunterladen

Datenquellen-Plug-Ins müssen in Windows Media Services Administrator konfiguriert werden, um diese zusätzlichen HTTP-Streaming-Szenarien zu unterstützen.

Informationen zum Protokoll-Rollover

Wenn Clients, die RTSP unterstützen, eine Verbindung zu einem Server herstellen, auf dem Windows Media® Services mit einem RTSP-URL-Moniker (z. B. rtsp://) oder einem MMS-URL-Moniker (z. B. mms://) ausgeführt wird, verwendet der Server einen Protokoll-Rollover, um den Inhalt an den Client zu streamen und so ein optimales Streaming-Erlebnis zu gewährleisten. Das automatische Protokoll-Rollover von RTSP/MMS auf RTSP mit UDP- oder TCP-basierten Transportnetzen (RTSPU oder RTSPT) oder sogar HTTP (wenn das WMS HTTP Server Control Protocol-Plug-in aktiviert ist) kann auftreten, wenn der Server versucht, das beste Protokoll auszuhandeln und dem Client ein optimales Streaming-Erlebnis zu bieten. Zu den Clients, die RTSP unterstützen, gehören Windows Media Player 9 Series oder höher oder andere Player, die das ActiveX-Steuerelement der Windows Media Player 9 Series verwenden.

Frühere Versionen von Windows Media Player, wie Windows Media Player für Windows XP, unterstützen das RTSP-Protokoll nicht, das MMS-Protokoll bietet jedoch Unterstützung für Protokoll-Rollover für diese Clients. Wenn also eine frühere Version des Players versucht, eine Verbindung zum Server über einen MMS-URL-Moniker herzustellen, kann die automatische Protokoll-Rollover-Funktion von MMS zu MMS mit UDP-basierten oder TCP-basierten Transporten (MMSU oder MMST) oder sogar HTTP (wenn das WMS HTTP Server Control Protocol-Plug-In aktiviert ist) auftreten, wenn der Server versucht, das beste Protokoll auszuhandeln und diesen Clients ein optimales Streaming-Erlebnis zu bieten.

Um sicherzustellen, dass Ihre Inhalte für alle Clients verfügbar sind, die eine Verbindung zu Ihrem Server herstellen, müssen Ports an Ihrer Firewall für alle Verbindungsprotokolle geöffnet werden, die innerhalb der Protokoll-Rollover-Funktion verwendet werden können.

Sie können Ihren Windows Media-Server zwingen, ein bestimmtes Protokoll zu verwenden, wenn Sie das Protokoll identifizieren, das in der Ankündigungsdatei verwendet werden soll (z. B. rtspu://server/publishing_point/file). Um ein optimales Streaming-Erlebnis für alle Client-Versionen zu gewährleisten, empfehlen wir, dass die URL das allgemeine MMS-Protokoll verwendet. Wenn Clients mit einer URL mit einem MMS-URL-Moniker eine Verbindung zu Ihrem Stream herstellen, erfolgt die erforderliche Protokoll-Rollover automatisch. Beachten Sie, dass Benutzer Streaming-Protokolle in den Eigenschafteneinstellungen von Windows Media Player deaktivieren können. Wenn ein Benutzer ein Protokoll deaktiviert, wird es im Rollover übersprungen. Wenn beispielsweise HTTP deaktiviert ist, werden die URLs nicht auf HTTP umgestellt.

Zuweisen von Ports für Windows Media-Dienste

Die meisten Firewalls dienen der Kontrolle des "eingehenden Datenverkehrs" zum Server. In der Regel steuern sie keinen "ausgehenden Datenverkehr" zu Clients. Ports in Ihrer Firewall für ausgehenden Datenverkehr können geschlossen werden, wenn in Ihrem Servernetzwerk strengere Sicherheitsrichtlinien implementiert werden. In diesem Abschnitt wird die standardmäßige Portzuweisung für Windows Media® Services für eingehenden und ausgehenden Datenverkehr (in den Tabellen als "Ein" und "Aus" angezeigt) beschrieben, sodass Sie alle Ports je nach Bedarf konfigurieren können.

In einigen Szenarien kann ausgehender Datenverkehr an einen Port einer Reihe verfügbarer Ports weitergeleitet werden. Die in den Tabellen gezeigten Portbereiche geben den gesamten Bereich der verfügbaren Ports an, Sie können jedoch innerhalb des Port-Bereichs weniger Ports zuweisen. Wenn Sie festlegen, wie viele Ports geöffnet werden sollen, müssen Sie Sicherheit mit Barrierefreiheit in Einklang bringen und nur genügend Ports öffnen, um allen Clients eine Verbindung zu ermöglichen. Bestimmen Sie zunächst, wie viele Ports Sie für Windows Media Services verwenden möchten, und öffnen Sie dann 10 Prozent mehr, um Überschneidungen mit anderen Programmen zu vermeiden. Nachdem Sie diese Nummer festgelegt haben, überwachen Sie Ihren Datenverkehr, um festzustellen, ob Anpassungen erforderlich sind.

Einschränkungen für den Portbereich können alle Anwendungen des Remote Procedure Calls (RPC) und des Distributed Component Object Model (DCOM) betreffen, die das System gemeinsam nutzen, nicht nur Windows Media Services. Wenn der zugewiesene Port-Bereich nicht breit genug ist, können Services von Mitbewerbern wie IIS mit Zufallsfehlern fehlschlagen. Der Port-Bereich muss für alle potenziellen Systemanwendungen geeignet sein, die RPC-, COM- oder DCOM-Dienste verwenden.

Um die Firewall-Konfiguration zu vereinfachen, können Sie jedes Serversteuerungsprotokoll-Plug-in (RTSP, MMS und HTTP) in Windows Media Services Administrator so konfigurieren, dass es einen bestimmten Port verwendet. Wenn Ihr Netzwerkadministrator bereits eine Reihe von Ports zur Verwendung durch Ihren Windows Media-Server geöffnet hat, können Sie diese Ports den Steuerungsprotokollen entsprechend zuweisen. Andernfalls können Sie den Netzwerkadministrator bitten, die Standard-Ports für jedes Protokoll zu öffnen. Wenn es nicht möglich ist, Ports auf Ihrer Firewall zu öffnen, können Windows Media Services Inhalte mit dem HTTP-Protokoll über Port 80 streamen.

Dies ist die standardmäßige Firewall-Portzuweisung für Windows Media Services, um einen Unicast-Stream bereitzustellen:

Anwendungsprotokoll	Protokoll	Port	Beschreibung
RTSP	TCP	554 (Ein/Aus)	Wird zum Akzeptieren eingehender RTSP-Client-Verbindungen und zum Senden von Datenpaketen an Clients verwendet, die RTSPT-Streaming verwenden.
RTSP	UDP	5004 (Aus)	Wird verwendet, um Datenpakete an Clients zu senden, die RTSPU-Streaming verwenden.

RTSP	UDP	5005 (Ein/Aus)	Wird verwendet, um Informationen über Paketverluste von Clients zu erhalten und Synchronisierungsinformationen für Clients bereitzustellen, die mit RTSPU streamen.
MMS	TCP	1755 (Ein/Aus)	Wird verwendet, um eingehende MMS-Clientverbindungen zu akzeptieren und Datenpakete an Clients zu senden, die mit MMST streamen.
MMS	UDP	1755 (Ein/Aus)	Wird verwendet, um Informationen über Paketverluste von Clients zu erhalten und Synchronisierungsinformationen für Clients bereitzustellen, die mit MMSU streamen.
MMS	UDP	1024 - 5000 (Aus)	Wird verwendet, um Datenpakete an Clients zu senden, die mit MMSU streamen. Öffnen Sie nur die erforderliche Anzahl von Ports.
HTTP	TCP	80 (Ein/Aus)	Wird verwendet, um eingehende HTTP-Clientverbindungen zu akzeptieren und Datenpakete an Clients zu senden, die HTTP-Streaming verwenden.

Um sicherzustellen, dass Ihre Inhalte für alle Clientversionen verfügbar sind, die mit Ihrem Server verbunden sind, öffnen Sie alle Ports, die in der Tabelle beschrieben sind, für alle Verbindungsprotokolle, die innerhalb des Protokoll-Rollovers verwendet werden können. Wenn Sie Windows Media Services auf einem Computer ausführen, auf dem Windows Server™ 2003 Service Pack 1 (SP1) ausgeführt wird, müssen Sie das Windows Media Services-Programm (wmserver.exe) als Ausnahme in der Windows-Firewall hinzufügen, um die standardmäßigen eingehenden Ports für Unicast-Streaming zu öffnen, anstatt Ports in der Firewall manuell zu öffnen.

Hinweis: Auf der Microsoft-Website erhalten Sie weitere Informationen zur MMS-Firewall-Konfiguration.

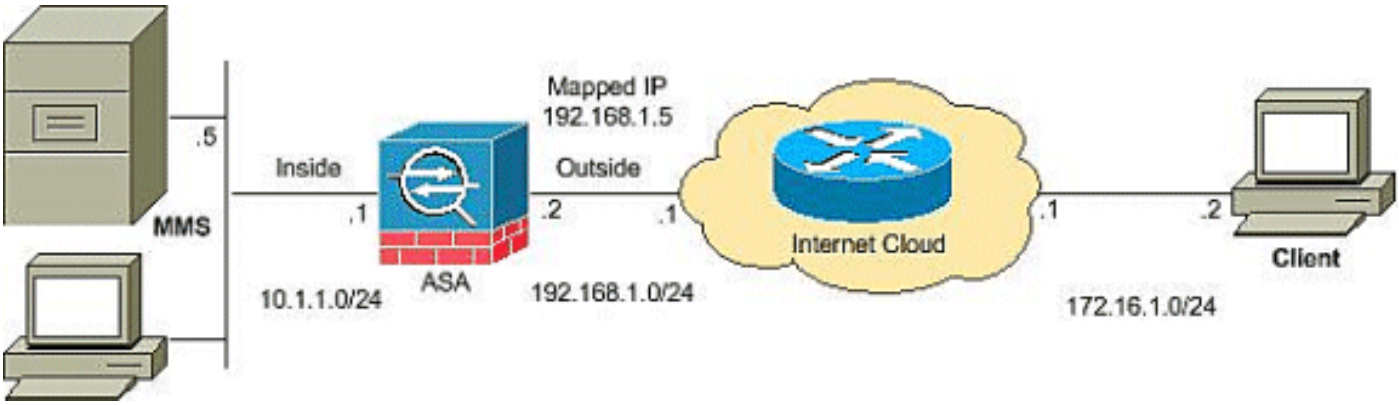
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Hinweis: Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Es handelt sich um RFC 1918-Adressen, die in einer Laborumgebung verwendet wurden.

Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

ASA-Konfiguration

```
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
```

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

- **Zugriffsliste anzeigen** - Zeigt die in ASA/PIX konfigurierten ACLs an.

```
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 anzeigen**): Zeigt NAT-Richtlinien und Zähler an.

```
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-StreamingProblembehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Inspect RTSP ist eine Standardkonfiguration auf der ASA. Er bricht den MMS-Datenverkehr, da die Sicherheits-Appliance keine NAT für RTSP-Nachrichten ausführen kann, da die eingebetteten IP-Adressen in den SDP-Dateien als Teil von HTTP- oder RTSP-Nachrichten enthalten sind. Pakete können fragmentiert werden, und die Sicherheits-Appliance kann NAT nicht für fragmentierte Pakete ausführen.

Problemumgehung: Dieses Problem kann behoben werden, wenn Sie die RTSP-Prüfung für diesen MMS-Datenverkehr wie folgt deaktivieren:

```
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
```

Zugehörige Informationen

- Cisco PIX Firewall-Software
- Cisco Secure PIX Firewall - Befehlsreferenzen
- Problemhinweise zu Sicherheitsprodukten (einschließlich PIX)
- Anforderungen für Kommentare (RFCs)
- Technischer Support - Cisco Systems
- Cisco ASA Support-Seite
- Technischer Support und Dokumentation - Cisco Systems