ASA/PIX: السماح لحركة مرور الشبكة بالوصول إلى خادم وسائط Microsoft (MMS) / دفق الفيديو من مثال تكوين الإنترنت

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين جهاز الأمان القابل للتكيف (ASA) للسماح للعميل أو المستخدم من الإنترنت بالوصول إلى خادم الوسائط (MMS) من Microsoft أو دفق الفيديو الذي تم وضعه في الشبكة الداخلية ل ASA.

المتطلبات الأساسية

المتطلبات

تأكد من استيفاء المتطلبات التالية قبل أن تحاول إجراء هذا التكوين:

- التكوين الأساسي ل ASA
- تم تكوين MMS ويعمل بشكل صحيح

المكونات المستخدمة

أسست المعلومة في هذا وثيقة على ال cisco ASA أن يركض برمجية صيغة x.7 وفيما بعد.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

المنتجات ذات الصلة

المعلومات الواردة في هذا المستند تنطبق أيضا على جدار حماية Cisco PIX الذي يشغل الإصدار x.7 من البرنامج والإصدارات الأحدث.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

معلومات جدار الحماية ل Windows Media Services 9 Series

إستخدام بروتوكولات الوسائط المتدفقة

تستخدم Microsoft® Windows Media® Services 9 Series بروتوكولي وسائط المتدفق لتوصيل المحتوى كبث أحادي إلى العملاء:

- بروتوكول الدفق في الوقت الفعلي (RTSP)
- بروتوكول (MMS Microsoft Media Server)

تدعم هذه البروتوكولات إجراءات التحكم بالعميل مثل إيقاف ملفات Windows Media المفهرسة وإيقافها مؤقتا وترحيلها وإعادة توجيهها بسرعة.

RTSP هو بروتوكول طبقة تطبيقات تم إنشاؤه خصيصا لتوفير التسليم المتحكم به لبيانات الوقت الفعلي، مثل محتوى الصوت والفيديو. يمكنك إستخدام RTSP لتدفق المحتوى إلى أجهزة الكمبيوتر التي تقوم بتشغيل Windows Media Player 9 Series أو إصدار أحدث، إلى العملاء الذين يستخدمون عنصر تحكم ActiveX® من Windows Media Player 9 Series أو إلى أجهزة الكمبيوتر الأخرى التي تعمل بنظام التشغيل Windows Media Services 9 Series. يعمل بروتوكول RTSP جنبا إلى جنب مع بروتوكول نقل الوقت الفعلي (RTP) لتنسيق حزم محتوى الوسائط المتعددة والتفاوض على بروتوكول طبقة النقل الأكثر فعالية، إما بروتوكول مخطط بيانات المستخدم (UDP) أو بروتوكول التحكم في النقل (TCP)، للاستخدام عند تسليم الدفق إلى العملاء. يمكنك تنفيذ RTSP من خلال المكون الإضافي لبروتوكول التحكم في خادم WMS RTSP في مسؤول خدمات الوسائط ل Windows. يتم تمكين هذه الإضافة بشكل افتراضي.

MMS هو بروتوكول طبقة تطبيق خاص تم تطويره لإصدارات سابقة من Windows Media Services. يمكنك إستخدام MMS لتدفق المحتوى إلى أجهزة الكمبيوتر التي تقوم بتشغيل Windows Media Player ل Windows® XP أو إصدار سابق. يمكنك تنفيذ MMS من خلال المكون الإضافي لبروتوكول التحكم في خادم WMS MMS في مسؤول خدمات الوسائط ل Windows. يتم تمكين هذه الإضافة بشكل افتراضي.

إستخدام HTTP

إذا تعذر فتح المنافذ الموجودة على جدار الحماية، فيمكن ل Windows Media® Services تدفق المحتوى باستخدام HTTP عبر المنفذ 80. يمكن إستخدام HTTP لتقديم التدفقات إلى جميع إصدارات Windows Media Player. يمكنك تنفيذ HTTP من خلال المكون الإضافي لبروتوكول التحكم في خادم WMS HTTP في مسؤول خدمات الوسائط ل Windows. لم يتم تمكين هذه الإضافة بشكل افتراضي. إن آخر خدمة، مثل إنترنت معلومة خدمات (IIS)، يستعمل ميناء 80 على ال نفسه عنوان، أنت يستطيع لا يمكن الإضافة.

كما يمكن إستخدام HTTP لما يلي:

- توزيع التدفقات بين خوادم Windows Media
- محتوى المصدر من جهاز تشفير Windows Media
- تنزيل قوائم التشغيل التي تم إنشاؤها ديناميكيا من خادم ويب

يجب تكوين إضافات مصدر البيانات في Windows Media Services Administrator لدعم سيناريوهات الدفق الإضافية ل HTTP.

حول تمرير البروتوكول

إذا قام العملاء الذين يدعمون RTSP بالاتصال بخادم يقوم بتشغيل Windows Media® Services باستخدام عنوان URL ل RTSP (على سبيل المثال، rtsp://) أو عنوان URL ل MMS (على سبيل المثال، mms://)، يستخدم الخادم إعادة توجيه البروتوكول لتدفق المحتوى إلى العميل لتوفير تجربة دفق مثالية. يمكن أن يحدث المرور التلقائي للبروتوكول من RTSP/MMS إلى RTSP باستخدام عمليات النقل المستندة إلى UDP أو RTSPU) TCP أو RTSPT) أو حتى HTTP (في حالة تمكين المكون الإضافي لبروتوكول التحكم في خادم WMS HTTP) عندما يحاول الخادم التفاوض على أفضل بروتوكول وتوفير تجربة دفق مثالية للعميل. يتضمن العملاء الذين يدعمون RTSP Windows Media Player 9 Series أو إصدار أحدث أو مشغلات أخرى تستخدم عنصر التحكم ActiveX من Windows Media Player 9 Series.

لا تدعم الإصدارات السابقة من Windows Media Player، مثل Windows Media Player ل Windows XP، بروتوكول RTSP، ولكن بروتوكول MMS يوفر دعم إعادة توجيه البروتوكول لهؤلاء العملاء. وبالتالي، عندما يحاول إصدار سابق من Player الاتصال بالخادم باستخدام أداة تحميل URL ل MMS، يمكن أن يحدث تمرير تلقائي للبروتوكول من MMS إلى MMS باستخدام عمليات النقل المستندة إلى UDP أو MMST، أو حتى HTTP (في حالة تمكين المكون الإضافي لبروتوكول التحكم في خادم WMS HTTP)، عندما يحاول الخادم التفاوض على أفضل بروتوكول وتوفير تجربة دفق مثالية لهؤلاء العملاء.

للتأكد من أن المحتوى الخاص بك متوفر لجميع العملاء المتصلين بالخادم الخاص بك، يجب فتح المنافذ الموجودة على جدار الحماية الخاص بك لجميع بروتوكولات الاتصال التي يمكن إستخدامها ضمن إعادة توجيه البروتوكول.

يمكنك فرض إستخدام خادم Windows Media لبروتوكول محدد في حالة التعرف على البروتوكول المطلوب إستخدامه في ملف الإعلان (على سبيل المثال، rtspu://server/publishing_point/file). لتوفير تجربة دفق مثالية لجميع إصدارات العملاء، نوصي باستخدام عنوان URL لبروتوكول MMS العام. إذا قام العملاء بالاتصال بالتدفق الخاص بك باستخدام عنوان URL الخاص ب MMS URL، فإن أي إعادة توجيه ضرورية للبروتوكول تحدث تلقائيا. كن على علم بأن المستخدمين يمكنهم تعطيل بروتوكولات الدفق في إعدادات خصائص Windows Media Player. إذا قام المستخدم بتعطيل بروتوكول، يتم تخطيه ضمن المرور الفوقي. على سبيل المثال، إذا تم تعطيل HTTP، فإن عناوين URL لا يتم تمريرها إلى HTTP.

تخصيص منافذ لخدمات وسائط Windows

يتم إستخدام معظم جدران الحماية للتحكم في "حركة المرور الواردة" إلى الخادم؛ ولا تتحكم بشكل عام في "حركة المرور الصادرة" للعملاء. يمكن إغلاق المنافذ الموجودة في جدار الحماية لحركة المرور الصادرة في حالة تنفيذ سياسة أمان أكثر صرامة على شبكة الخادم. يصف هذا القسم تخصيص المنفذ الافتراضي لخدمات Windows Media® لكل من حركة المرور الواردة والصادرة (تظهر ك "داخل" و"خارج" في الجداول) حتى يمكنك تكوين جميع المنافذ حسب الحاجة.

في بعض السيناريوهات، يمكن توجيه حركة المرور الصادرة إلى منفذ واحد في نطاق من المنافذ المتاحة. تشير نطاقات المنافذ الموضحة في الجداول إلى النطاق الكامل للمنافذ المتاحة، ولكن يمكنك تخصيص منافذ أقل داخل نطاق المنفذ. عندما تحدد عدد المنافذ التي سيتم فتحها، وازن بين التأمين وإمكانية الوصول، وافتح المنافذ الكافية فقط للسماح لكل العملاء بإجراء اتصال. أولا، حدد عدد المنافذ التي تتوقع إستخدامها ل Windows Media Services، ثم افتح 10 بالمائة أكثر لحساب التداخل مع البرامج الأخرى. بعد تحديد هذا الرقم، راقب حركة المرور لتحديد ما إذا كان من الضروري إجراء أي تعديلات.

من المحتمل أن تؤثر قيود نطاق المنفذ على كافة إستدعاءات الإجراء البعيد (RPC) وتطبيقات نموذج كائن المكون الموزع (DCOM) التي تشارك النظام، وليس فقط على خدمات Windows Media. إذا لم يكن نطاق المنفذ المخصص واسعا بما يكفي، فقد تفشل الخدمات التنافسية مثل IIS مع حدوث أخطاء عشوائية. يجب أن يكون نطاق المنفذ قادرا على إستيعاب جميع تطبيقات النظام المحتملة التي تستخدم خدمات RPC أو COM أو DCOM.

لجعل تكوين جدار الحماية أكثر سهولة، يمكنك تكوين المكون الإضافي لكل بروتوكول تحكم خادم (RTSP و MMS و HTTP) في Windows Media Services Administrator لاستخدام منفذ معين. إذا كان مسؤول الشبكة قد قام بالفعل بفتح سلسلة من المنافذ لاستخدامها من قبل خادم Windows Media، فيمكنك تخصيص تلك المنافذ لبروتوكولات التحكم وفقا لذلك. وإذا لم تكن هناك مساحة، فيمكنك الطلب من مسؤول الشبكة فتح المنافذ الافتراضية لكل بروتوكول. إذا لم يكن من الممكن فتح منافذ على جدار الحماية الخاص بك، فيمكن ل Windows Media Services دفق المحتوى باستخدام بروتوكول HTTP عبر المنفذ 80.

هذا هو تخصيص منفذ جدار الحماية الافتراضي ل Windows Media Services لتوفير تدفق أحادي البث:

بروتوكول التطبيق	البروتوكول	المنفذ	الوصف
RTSP	TCP	554 (دخل/خرج)	يستخدم لقبول إتصالات عميل RTSP الواردة ولتسليم حزم البيانات إلى العملاء المتدفقة باستخدام RTSPT.
RTSP	UDP	5004 (خارج)	يستخدم لتسليم حزم البيانات إلى العملاء المتدفقة باستخدام RTSPU.
RTSP	UDP	5005	يستخد

		(الإدخال/الإخراج)	م لاستلام معلومات فقدان الحزمة من العملاء وتوفير معلومات المزامنة للعملاء الذين يتم دفقهم باستخدام RTS.PU.
MMS	TCP	1755 (دخل/خرج)	يستخدم لقبول إتصالات عميل MMS الواردة ولتسليم حزم البيانات إلى العملاء المتدفقين باستخدام MMS.T.
MMS	UDP	1755 (دخل/خرج)	يستخدم لتلقي معلومات عن فقد الحزم من

			العملاء وتوفير معلومات المزامنة للعملاء المتدفقين باستخدام MMSU.
MMS	UDP	1024-5000 (خارج)	يستخدم لتسليم حزم البيانات إلى العملاء المتدفقين باستخدام MMSU. افتح فقط العدد الضروري من ميناء.
HTTP	TCP	80 (دخل/خرج)	يستخدم لقبول إتصالات عميل HTTP الواردة ولتسليم حزم البيانات إلى العملاء المتدفق

			قة باستخدام HTTP.

للتأكد من أن المحتوى الخاص بك متوفر لجميع إصدارات العملاء المتصلة بالخادم الخاص بك، افتح جميع المنافذ الموضحة في الجدول لجميع بروتوكولات الاتصال التي يمكن إستخدامها ضمن إعادة توجيه البروتوكول. إذا قمت بتشغيل Windows Media Services على جهاز كمبيوتر يعمل بنظام التشغيل Windows Server™ 2003 (Service Pack 1 (SP1)، فيجب عليك إضافة برنامج (wmserver.exe Windows Media Services) كإستثناء في جدار حماية Windows لفتح المنافذ الواردة الافتراضية لتدفق البث الأحادي، بدلا من فتح المنافذ في جدار الحماية يدويا.

ملاحظة: ارجع إلى موقع Microsoft على الويب لمعرفة المزيد حول تكوين جدار حماية MMS.

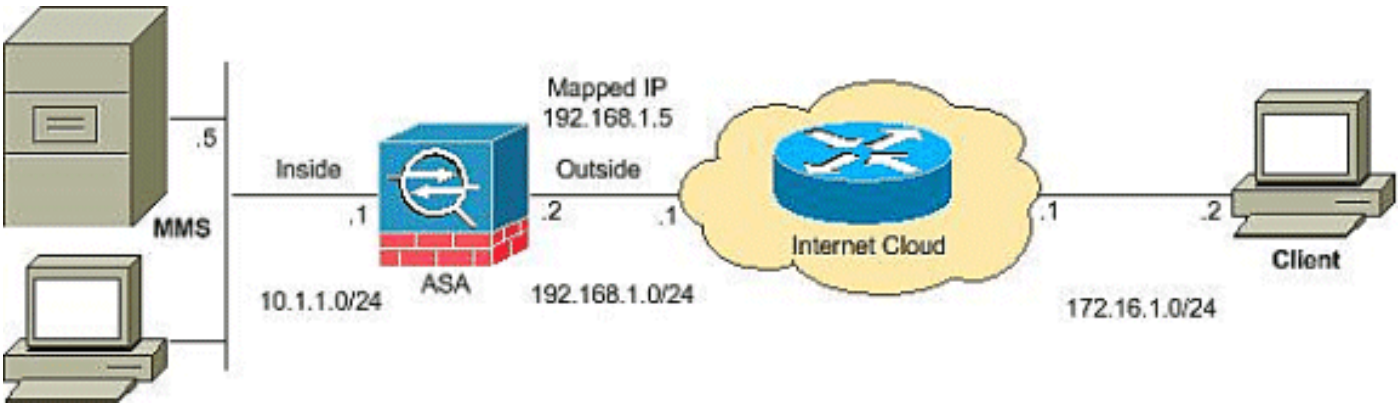
التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



ملاحظة: ال ip ليس يخاطب خطة يستعمل في هذا تشكيل قانونيا routable على الإنترنت. هم rfc 1918 عنوان أن يتلقى يكون استعملت في مختبر بيئة.

التكوينات

يستخدم هذا المستند التكوينات التالية:

تكوين 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
eq 1755 192.168.1.5
Command to open the MMS udp port access-list ---!
outside_access_in extended permit tcp any host
eq 1755 192.168.1.5
Command to open the MMS tcp port access-list ---!
outside_access_in extended permit udp any host
eq 5005 192.168.1.5
Command to open the RTSP udp port access-list ---!
outside_access_in extended permit tcp any host
eq www 192.168.1.5
Command to open the HTTP port access-list ---!
outside_access_in extended permit tcp any host
eq rtsp 192.168.1.5
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
```

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر show. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر show .

- show access-list—يعرض قوائم التحكم في الوصول (ACL) التي تم تكوينها في 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
```

- **عرض nat**—يعرض سياسات NAT وعدادات.

```
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
```

أستكشاف أخطاء الفيديو وإصلاحها المتدفق

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

فحص RTSP هو تكوين افتراضي على ASA. وهو يفكك حركة مرور MMS لأن جهاز الأمان لا يمكنه تنفيذ NAT على رسائل RTSP لأن عناوين IP المضمنة موجودة في ملفات SDP كجزء من رسائل HTTP أو RTSP. يمكن أن تكون الحزم مجزأة، ولا يمكن أن يقوم جهاز الأمان بتنفيذ NAT على الحزم المجزأة.

الحل البديل: يمكن حل هذه المشكلة إذا قمت بتعطيل فحص RTSP لحركة مرور MMS المحددة هذه كما هو موضح:

```
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
```

معلومات ذات صلة

- برنامج جدار حماية Cisco PIX
- مراجع أوامر جدار حماية PIX الآمن من Cisco
- الإعلامات الميدانية لمنتج الأمان (بما في ذلك PIX)
- طلبات التعليقات (RFCs)
- الدعم الفني - Cisco Systems
- صفحة دعم ASA من Cisco

- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).