ASA/PIX：インターネットからのネットワーク トラフィックを許可して Microsoft メディア サーバ（MMS）/ストリーミング ビデオにアクセスする設定例

内容

概要

このドキュメントでは、適応型セキュリティ アプライアンス（ASA）の内部ネットワークに配置された Microsoft メディア サーバ（MMS）またはストリーミング ビデオへクライアントまたはユーザがインターネットからアクセスできるように ASA を設定する方法について説明します。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- ASA に関する基本的設定
- MMS の設定と正常な動作

使用するコンポーネント

このドキュメントの情報は、ソフトウェア バージョン 7.x 以降が稼働する Cisco ASA に基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

関連製品

このドキュメントの情報は、ソフトウェア バージョン 7.x 以降が稼働する Cisco PIX ファイアウォールにも適用できます。

表記法

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

Windows Media Services 9 シリーズのファイアウォールに関する情報

ストリーミング メディア プロトコルの使用

Microsoft® Windows Media® サービス9シリーズは、次の2つのストリーミングメディアプロトコルを使用して、コンテンツをユニキャストストリームとしてクライアントに配信します。

- リアルタイム ストリーミング プロトコル（RTSP）
- Microsoft メディア サーバ（MMS）プロトコル

これらプロトコルは、インデックスが付けられた Windows Media ファイルに対する停止、一時停止、巻き戻し、早送りなどのクライアント制御機能をサポートします。

RTSP は、音声やビデオ コンテンツなどのリアルタイム データを配信制御するために特別に作成されたアプリケーション レイヤ プロトコルです。RTSPを使用して、Windows Media Player 9シリーズ以降を実行するコンピュータ、Windows Media Player 9シリーズActiveX®コントロールを使用するクライアント、またはWindows Media Services 9シリーズを実行する他のコンピュータにコンテンツをストリーミングできます。RTSP は、リアルタイム転送プロトコル（RTP）と連携してマルチメディア コンテンツのパケットをフォーマットし、クライアントへのストリーミング時にユーザ データグラム プロトコル（UDP）とトランスポート制御プロトコル（TCP）のうち、より効率的ないずれかのトランスポート レイヤ プロトコルをネゴシエートします。RTSP は、Windows Media Services アドミニストレータ内の WMS RTSP サーバ制御プロトコル プラグインから実装できます。このプラグインはデフォルトで有効になっています。

MMS は、Windows Media Services の前のバージョンで開発された独自のアプリケーション レイヤ プロトコルです。MMSを使用して、Windows Media Player for Windows® XP以前を実行するコンピュータにコンテンツをストリーミングできます。MMS は、Windows Media Services アドミニストレータ内の WMS MMS サーバ制御プロトコル プラグインから実装できます。このプラグインはデフォルトで有効になっています。

HTTP の使用

ファイアウォール上のポートを開くことができない場合、Windows Media® Servicesはポート80経由でHTTPでコンテンツをストリーミングできます。HTTPを使用して、すべてのWindows Media Playerバージョンにストリームを配信できます。HTTP は、Windows Media Services アドミニストレータ内の WMS HTTP サーバ制御プロトコル プラグインから実装できます。このプラグインはデフォルトで有効になっていません。Internet Information Services (IIS) などの他のサービスが同じ IP アドレスでポート 80 を使用している場合は、このプラグインを有効にできません。

このほか、HTTP は次の用途で利用できます。

- Windows Media サーバ間でストリーミング配信する
- Windows Media エンコーダからコンテンツを調達する
- 動的に生成されたプレイリストを Web サーバからダウンロードする

これらの HTTP ストリーミング シナリオをサポートする場合は、Windows Media Services アドミニストレータでデータ ソース プラグインを設定する必要があります。

プロトコル ロールオーバーについて

Windows Media® Services が稼働するサーバに対して RTSP 接続をサポートするクライアントが、RTSP URL モニカ (rtsp:// など) または MMS URL モニカ (mms:// など) を使用してアクセスするとき、サーバは最適なストリーミング エクスペリンスを実現するためにプロトコル ロールオーバーでクライアントへコンテンツをストリーミングします。サーバは、クライアントの最適なストリーミング エクスペリンスを実現するために適したプロトコルをネゴシエートします。このとき、UDP ベース転送または TCP ベース転送 (RTSPU または RTSPT)、あるいは (WMS HTTP サーバ制御プロトコル プラグインが有効な場合に) HTTP を使用して、RTSP/MMS から RTSP に対する自動プロトコル ロールオーバーが発生することがあります。RTSP をサポートするクライアントには、Windows Media Player 9 シリーズ以降、または Windows Media Player 9 シリーズ ActiveX コントロールが含まれます。

Windows Media Player for Windows XP などの以前の Windows Media Player バージョンでは、RTSP プロトコルをサポートしていません。ただし、これらのクライアントには MMS プロトコルがプロトコル ロールオーバーを提供します。したがって、以前の Windows Media Player が MMS URL モニカを使用してサーバに接続を試みた場合、サーバが最適なプロトコルをネゴシエートして、これらのクライアントに最適なストリーミング エクスペリンスを提供しようと試みたとき、MMS は UDP ベース転送または TCP ベース転送 (MMSU または MMST)、あるいは (WMS HTTP サーバ制御プロトコル プラグインが有効な場合に) HTTP を使用して、MMS から MMS に対する自動プロトコル ロールオーバー発生することがあります。

サーバに接続されたすべてのクライアントにコンテンツを配信するには、プロトコル ロールオーバーで使用する接続プロトコルすべてに対してファイアウォールのポートを開放する必要があります。

アナウンスメント ファイル (rtspu://server/publishing_point/file など) で用いられているプロトコルがわかる場合は、Windows Media サーバで特定のプロトコルを使用するように強制できます。すべてのクライアントのバージョンで最適なストリーミング エクスペリンスを実現するためにも、URL では一般的な MMS プロトコルの使用することを推奨します。クライアントが MMS URL モニカの URL からストリームに接続すると、必要なプロトコル ロールオーバーが自動的に実行されます。なお、ユーザは Windows Media Player のプロパティ設定でストリーミング プロトコルを無効にできる点にご注意ください。ユーザがプロトコルを無効に設定していると、ロールオーバーはスキップされます。たとえば、HTTP が無効な場合、URL は HTTP にロールオーバーさ

れません。

Windows Media Services へのポート割り当て

ほとんどのファイアウォールは、サーバへの「着信トラフィック」を制御するために使用されています。つまり、一般的にはクライアントへの「発信トラフィック」を制御しないということです。ファイアウォールの発信トラフィック用ポートは、より強固なセキュリティ ポリシーがサーバ ネットワークで実装されている場合に、閉じていることがあります。このセクションでは、すべてのポートを必要に応じて設定できるように、Windows Media®サービスの着信トラフィックと発信トラフィックの両方（表の「In」および「Out」として示されます）のデフォルトのポート割り当てを説明します。

一部のシナリオでは、発信トラフィックを利用可能なポート範囲のうちの 1 つに宛てることができます。表のポート範囲は、利用可能な全範囲を示しています。もちろん、ポート範囲よりも少ないポートに割り当てても問題はありません。開放するポート数を決定するときは、アクセシビリティとセキュリティのバランスを考えて、すべてのクライアントが接続するために十分な数だけ開放するようにします。最初に、Windows Media Services で使用する予定のポート数を決定し、その他のプログラムとのオーバーラップを想定して、さらに 10 % 多い数のポートを開放します。ポート数が決まったら、トラフィックをモニタして必要な調整があるかどうかを確認します。

ポート範囲に制限があると、Windows Media Services だけでなく、システムを共有するリモート プロシージャ コール（RPC）や分散コンポーネント オブジェクト モデル（DCOM）アプリケーションのすべてに影響が及びます。割り当てたポート範囲が十分でないと、IIS などの競合サービスがランダム エラーにより失敗する可能性があります。ポート範囲は、RPC、COM、または DCOM サービスを使用する可能性のあるすべてのシステム アプリケーションに対応できるよう、十分に幅をとっておく必要があります。

Windows Media Services アドミニストレータのサーバ制御プロトコル プラグイン（RTSP、MMS、HTTP）をそれぞれ設定して特定のポートを使用すると、簡単にファイアウォールを設定することができます。すでにネットワーク管理者が Windows Media サーバ用に一連のポートを開放している場合は、これらのポートを制御プロトコルへ適宜割り当てられます。まだ開放されていない場合は、ネットワーク管理者に各プロトコルのデフォルト ポートを開放するように依頼します。万一ポートを開放できない場合、Windows Media Services では、ポート 80 で HTTP プロトコルを使用してコンテンツをストリーミングできます。

次に、ユニキャスト ストリームを配信するために Windows Media Services 向けに割り当てられたデフォルトのファイアウォール ポートを示します。

アプリケーション プロトコル	プロトコル	ポート	説明
RTSP	TCP	554（着信/発信）	クライアント接続の着信 RTSP を許可し、RTSPT でストリーミングするクライアント宛てにデータ パケットを配信する場合に使用します。
RTSP	UDP	5004（発信）	RTSPU でストリーミングするクライアント宛てにデータ パケットを配信する場合に使用します。

RTSP	UDP	5005（着信/発信）	クライアントからのパケット損失情報を受信し、RTSPU でストリーミングするクライアント宛てに同期情報を提供する場合に使用します。
MMS	TCP	1755（着信/発信）	クライアント接続の着信 MMS を許可し、MMST でストリーミングするクライアント宛てにデータ パケットを配信する場合に使用します。
MMS	UDP	1755（着信/発信）	クライアントからのパケット損失情報を受信し、MMSU でストリーミングするクライアント宛てに同期情報を提供する場合に使用します。
MMS	UDP	1024 ～ 5000（発信）	NMSU でストリーミングするクライアント宛てにデータ パケットを配信する場合に使用します。必要なポート数のみを開放します。
HTTP	TCP	80（In/Out）	クライアント接続の着信 HTTP を許可し、HTTP でストリーミングするクライアント宛てにデータ パケットを配信する場合に使用します。

サーバに接続されたすべてのクライアント バージョンに対してコンテンツを配信できるようにするには、プロトコル ロールオーバーで使用可能な接続プロトコルすべてに対して、表に示された全ポートを開放する必要があります。Windows Server™ 2003 Service Pack 1（SP1）が稼働するコンピュータ上で Windows Media Services を実行する場合、手動でファイアウォールのポートを開放するのではなく、Windows ファイアウォールに Windows Media Services プログラム（wmserver.exe）を例外として追加し、ユニキャスト ストリーミング用にデフォルトの着信ポートを開放します。

注：MMSファイアウォールの設定に関する詳細については 、MicrosoftのWebサイトを参照してください。

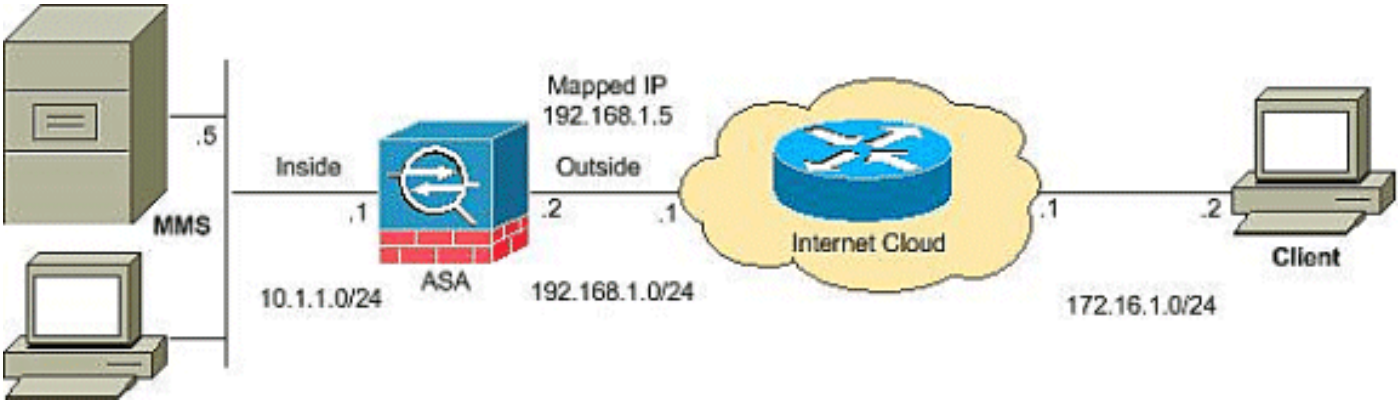
設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことをご了承ください。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



注：この設定で使用されるIPアドレッシング方式は、インターネット上で正式にルーティング可能なものではありません。これらは RFC 1918 で使用されているアドレスであり、ラボ環境で使用されたものです。

設定

このドキュメントでは、次の構成を使用します。

ASA の設定

```
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
```

確認

ここでは、設定が正常に機能しているかどうかを確認します。

アウトプット インタープリタ ツール（登録ユーザ専用）（OIT）は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

- **Show access-list**—：ASA/PIX 内で設定された ACL を表示します。

```
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 ポリシーとカウンターを表示します。

```
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
```

ストリーミング ビデオのトラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

RTSP が ASA でデフォルト設定されているか検査します。セキュリティ アプライアンスでは、埋め込み IP アドレスが HTTP メッセージまたは RTSP メッセージの一部として SDP ファイルに含まれているので、RTSP メッセージ上で NAT を実行できずに、MMS トラフィックが切断されます。また、セキュリティ アプライアンスはフラグメント化されたパケット上で NAT を実行できません。

回避策：この問題は、次に示す特定の MMS トラフィックで RTSP 検査をディセーブルにすると回避できます。

```
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
```

関連情報

- Cisco PIX Firewall ソフトウェア
- Cisco Secure PIX ファイアウォール コマンド リファレンス
- セキュリティ製品に関する Field Notice (PIX を含む)
- Requests for Comments (RFCs)
- テクニカルサポート - Cisco Systems
- Cisco ASA に関するサポート ページ
- テクニカル サポートとドキュメント – Cisco Systems