PIX/ASA 7.x： FTP/TFTP サービスの有効化の設定例

目次

概要

このドキュメントでは、ネットワークの Outside に居るユーザが DMZ ネットワーク内の FTP と TFTP のサービスにアクセスするために必要な手順を説明しています。

File Transfer Protocol (FTP)

FTP には 2 つの形式があります。

- アクティブ モード
- パッシブ モード

アクティブ FTP モードでは、クライアントがランダムな非特権ポート (N>1023) から FTP サーバのコマンド ポート (21) へ接続します。 次に、クライアントによるポート N+1 のリスニングが開始され、FTP コマンド ポート N+1 が FTP サーバへ送信されます。 次に、サーバによってローカルのデータ ポート (ポート 20) からクライアントの指定されたデータ ポートへ再度接続が行われます。

パッシブ FTP モードでは、クライアントによってサーバへの接続がどちらも開始され、サーバからクライアントへの着信データ ポート接続に対するフィルタリングが行われるファイアウォールの問題が解決されます。 FTP 接続が開かれると、クライアントによって 2 つのランダムな非特権ポートがローカルに開かれます（N>1023 および N+1）。 最初のポートからポート 21 上でサーバに接続されます。 ただし、この後で **port** コマンドを発行して、そのデータ ポートへのサーバの接続を許可する代わりに、クライアントから **PASV** コマンドが発行されます。 この結果、サーバによってランダムな非特権ポート（P>1023）が開かれ、**port P** コマンドがクライアントへ送信されます。 次に、データを転送するために、クライアントによってサーバ上でポート N+1 からポート P への接続が開始されます。 セキュリティ アプライアンスで **inspection** コマンドが設定されていない場合、Inside ユーザからのアウトバウンドに向けた FTP はパッシブ モードでのみ動作します。 また、FTP サーバへのインバウンドに向けた Outside ユーザは、アクセスを拒否されます。

バージョン 8.3 以降の Cisco Adaptive Security Appliance（ASA）での ASDM を使用した同等な設定の詳細について『ASA 8.3.x 以降： バージョン 8.3 および それ 以降との Cisco 適応型セキュリティ アプライアンス（ASA）ソフトウェアの ASDM を使用して同一の構成に関する詳細については FTP/TFTP サービス 設定例を（ASA）有効に して下さい。

Trivial File Transfer Protocol（TFTP）

RFC 1350 で記述されるように、TFTP は、TFTP サーバとクライアントの間でファイルの読み書きを行うための単純なプロトコルです。 TFTP では、UDP ポート 69 が使用されます。

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。

- 必要なインターフェイス間で基本的な通信が存在する。
- DMZ ネットワークの Inside に配置された、設定済みの FTP サーバが存在する。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- 7.2(2) ソフトウェア イメージが稼働する ASA 5500 シリーズ適応型セキュリティ アプライアンス
- FTP サービスが稼働する Windows 2003 Server
- TFTP サービスが稼働する Windows 2003 Server
- ネットワークの Outside に配置されたクライアント PC

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たものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。

注: この設定で使用している IP アドレス スキームは、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。 これらはラボ環境で使用された RFC 1918 でのアドレスです。

関連製品

この設定は、PIX セキュリティ アプライアンス 7.x にも使用できます。

表記法

ドキュメント表記の詳細は、『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。

背景説明

セキュリティ アプライアンスは、アダプティブ セキュリティ アルゴリズム機能によって、アプリケーション検査をサポートしています。 アダプティブ セキュリティ アルゴリズムで使用されるアプリケーションのステートフル インスペクションによって、セキュリティ アプライアンスは、ファイアウォールを通過する各コネクションをトラッキングし、これらのコネクションが有効であることを確認します。 また、ファイアウォールはステートフル インスペクションによってコネクションの状態も監視し、状態テーブルに情報を格納します。 管理者定義のルールに加えて状態テーブルを使用することで、フィルタリングの決定が、過去にファイアウォールを通過したパケットによって確立されたコンテキスト情報に基づいて行われるようになります。 アプリケーション検査の実装は、次の処理で構成されています。

- トラフィックを識別する。
- トラフィックに検査を適用する。
- インターフェイス上での検査をアクティブ化する。

高度なプロトコル処理

FTP

一部のアプリケーションでは、Cisco セキュリティ アプライアンス アプリケーションの検査機能による特別な処理が必要です。 これらのタイプのアプリケーションでは、通常、IP アドレッシング情報がユーザ データ パケットに埋め込まれるか、動的に割り当てられたポートにセカンダリ チャネルが開かれます。 アプリケーション検査機能は、Network Address Translation (NAT; ネットワーク アドレス変換) とも共に動作し、埋め込まれたアドレッシング情報の場所を識別するのに役立ちます。

埋め込みのアドレッシング情報の識別に加えて、アプリケーション検査機能ではセッションが監視され、セカンダリ チャネルのポート番号が判断されます。 多くのプロトコルによってセカンダリの TCP ポートまたは UDP ポートが開かれ、パフォーマンスが向上します。 既知のポートで初期セッションが使用され、動的に割り当てられたポート番号がネゴシエーションされます。 アプリケーション検査機能では、これらのセッションが監視され、動的なポート割り当てが識別され、特定のセッションの間にこれらのポートでのデータ交換が許可されます。 このような動作は、マルチメディアおよび FTP のアプリケーションでみられます。

FTP プロトコルでは、FTP セッションごとに 2 つのポートを使用するために、特別な処理が必要です。 FTP プロトコルでは、データの転送がアクティブになった場合、 それぞれポート 21 を使用するコントロール チャネルとポート 20 を使用するデータ チャネルの 2 つのポートが使用されます。 コントロール チャネルを介して FTP セッションを開始するユーザは、そのチャネルを介

してすべてのデータ要求を行います。 次に、FTP サーバによって要求が開始され、サーバ ポート 20 からユーザのコンピュータへポートが開かれます。 FTP では、データ チャネル通信のために常にユーザ ポート 20 が使用されます。 FTP 検査がセキュリティ アプライアンスでイネーブルになっていない場合、この要求は廃棄され、FTP セッションでは要求されたデータが転送されません。 FTP 検査がセキュリティ アプライアンスでイネーブルになっている場合、セキュリティ アプライアンスによってコントロール チャネルが監視され、データ チャネルを開く要求が認識されます。 FTP プロトコルによって、データ チャネル ポート番号の詳細がコントロール チャネル トラフィックに埋め込まれると、セキュリティ アプライアンスによるデータ ポート変更に対するコントロール チャネルの検査が必要になります。 セキュリティ アプライアンスによって要求が認識されると、データ チャネル トラフィック用の窓口が一時的に開かれますが、これはセッションの間中、開かれたままです。 この方法で、FTP 検査機能によってコントロール チャネルが監視され、データ ポートの割り当てが識別され、セッションの間中、データ ポートでのデータ交換が許可されます。

セキュリティ アプライアンスによって、デフォルトではグローバル検査クラスマップを経由して FTP トラフィックのポート 21 の接続が検査されます。 また、セキュリティ アプライアンスでは、アクティブとパッシブの FTP セッションの間での差異が認識されます。 FTP セッションではパッシブ FTP データ転送がサポートされますが、セキュリティ アプライアンスでは **inspect ftp** コマンドを介してユーザからのデータ ポート要求が認識され、1023 より大きい番号の新規データ ポートが開かれます。

FTP アプリケーション検査によって、FTP セッションが検査され、次の 4 つのタスクが実行されます。

- 動的なセカンダリ データ接続の準備
- FTP コマンド応答シーケンスの追跡
- 監査証跡の生成
- NAT を使用した埋め込み IP アドレスの変換

FTP アプリケーション検査によって、FTP データ転送のセカンダリ チャネルが準備されます。 ファイルのアップロード、ファイルのダウンロード、またはディレクトリ リストのイベントに応答してチャネルが割り当てられますが、これらのチャネルは事前にネゴシエートされる必要があります。 ポートは、**PORT** コマンド、または **PASV** (227) コマンドを介してネゴシエートされます。

TFTP

TFTP 検査はデフォルトでイネーブルになっています。

セキュリティ アプライアンスによって TFTP トラフィックが検査され、必要に応じて TFTP クライアントとサーバの間でのファイル転送を許可するために connection と nat(pat) 変換が動的に作成されます。 具体的には、インスペクション エンジンによって TFTP 読み取り要求 (RRQ)、書き込み要求 (WRQ)、および エラー通知 (ERROR) が検査されます。

動的なセカンダリ チャネルと PAT 変換は、必要に応じて有効な RRQ または WRQ の受信時に割り当てられます。 その後、このセカンダリ チャネルはファイル転送または エラー通知のために TFTP によって使用されます。

セカンダリ チャネルを介したトラフィックを開始することができるのは TFTP サーバだけであり、TFTP クライアントとサーバの間に不完全なセカンダリ チャネルが最大で 1 つだけ存在できます。 サーバからの エラー通知によって、セカンダリ チャネルが閉じられます。

TFTP トラフィックをリダイレクトするためにスタティック PAT が使用される場合は、TFTP 検

査をイネーブルにする必要があります。

基本的な FTP アプリケーション検査の設定

デフォルトでは、デフォルトのアプリケーション検査トラフィックをすべて照合する 1 つのポリシー（グローバル ポリシー）が設定に含まれており、これによりすべてのインターフェイス上のトラフィックに検査が適用されます。 デフォルトのアプリケーション検査トラフィックには、各プロトコルのデフォルトのポートに対するトラフィックが含まれています。 適用できるグローバル ポリシーは 1 つだけなので、グローバル ポリシーを変更する場合、たとえば、非標準ポートに検査を適用したり、デフォルトではイネーブルになっていない検査を追加したりする場合は、デフォルトのポリシーを編集するか、またはデフォルトのポリシーをディセーブルにしてから新しいポリシーを適用する必要があります。 すべてのデフォルトのポートのリストについては、『デフォルトの検査ポリシー』を参照してください。

1. **policy-map global_policy** コマンドを発行します。`ASAwAIP-CLI(config)#policy-map global_policy`
2. **class inspection_default** コマンドを発行します。`ASAwAIP-CLI(config-pmap)#class inspection_default`
3. **inspect FTP** コマンドを発行します。`ASAwAIP-CLI(config-pmap-c)#inspect FTP` **inspect FTP strict** コマンドを使用するオプションが用意されてます。 このコマンドでは、FTP 要求に埋め込まれたコマンドの Web ブラウザによる送信を回避することで、保護されたネットワークのセキュリティが向上します。インターフェイス上で **strict** オプションを有効にすると、FTP 検査によって次の手順が適用されます。セキュリティ アプライアンスによって新しいコマンドが許可されるには、FTP コマンドが確認応答される必要がある。セキュリティ アプライアンスによって、埋め込まれたコマンドが送信される接続が廃棄される。**227** コマンドおよび **PORT コマンド**がチェックされ、これらがエラー文字列に表示されていないことが確認される。**警告： strict** オプションを使用すると、FTP の RFC に厳密に準拠していない FTP クライアントでは失敗することになる可能性があります。 **strict** オプションの使用についての詳細は、『strict オプションの使用』を参照してください。

設定例

デバイス名 1

```
ASA-AIP-CLI(config)#show running-config ASA Version
7.2(2) ! hostname ASA-AIP-CLI domain-name corp.com
enable password WwXYvtKrnjXqGbu1 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 ! interface Ethernet0/2 nameif
DMZ security-level 50 ip address 172.16.1.12
255.255.255.0 ! interface Ethernet0/3 no nameif no
security-level no ip address ! interface Management0/0
no nameif no security-level no ip address ! !--- Output
is suppressed. !--- Permit inbound FTP control traffic.
access-list 100 extended permit tcp any host 192.168.1.5
eq ftp !--- Permit inbound FTP data traffic. access-list
100 extended permit tcp any host 192.168.1.5 eq ftp-data
! !--- Command to redirect the FTP traffic received on
IP 192.168.1.5 !--- to IP 172.16.1.5. static
(DMZ,outside) 192.168.1.5 172.16.1.5 netmask
255.255.255.255 access-group 100 in interface outside
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
inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! !---
This command tells the device to !--- use the
"global_policy" policy-map on all interfaces. service-
policy global_policy global prompt hostname context
Cryptochecksum:4b2f54134e685d11b274ee159e5ed009 : end
ASA-AIP-CLI(config)#
```

標準外 TCP ポートでの FTP プロトコル検査の設定

次の設定を使用して、標準外 TCP ポートで FTP プロトコル検査を設定できます（XXXX を新規のポート番号で置き換えてください）。

```
access-list ftp-list extended permit tcp any any eq XXXX
!
class-map ftp-class
  match access-list ftp-list
!
policy-map global_policy
  class ftp-class
   inspect ftp
```

基本的な TFTP アプリケーション インスペクションの設定

デフォルトでは、デフォルトのアプリケーション検査トラフィックをすべて照合する 1 つのポリシー（グローバル ポリシー）が設定に含まれており、これによりすべてのインターフェイス上のトラフィックに検査が適用されます。 デフォルトのアプリケーション検査トラフィックには、各プロトコルのデフォルトのポートに対するトラフィックが含まれています。 適用できるグローバル ポリシーは 1 つだけです。 したがって、グローバル ポリシーを変更する場合、たとえば、非標準ポートに検査を適用したり、デフォルトではイネーブルになっていない検査を追加したりする場合は、デフォルトのポリシーを編集するか、またはデフォルトのポリシーをディセーブルにしてから新しいポリシーを適用する必要があります。 すべてのデフォルトのポートのリストについては、『デフォルトの検査ポリシー』を参照してください。

1. **policy-map global_policy** コマンドを発行します。`ASAwAIP-CLI(config)#policy-map global_policy`
2. **class inspection_default** コマンドを発行します。`ASAwAIP-CLI(config-pmap)#class inspection_default`
3. **inspect TFTP** コマンドを発行します。`ASAwAIP-CLI(config-pmap-c)#inspect TFTP`

設定例

デバイス名 1

```
ASA-AIP-CLI(config)#show running-config ASA Version
7.2(2) ! hostname ASA-AIP-CLI domain-name corp.com
enable password WwXYvtKrnjXqGbu1 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 ! interface Ethernet0/2 nameif
DMZ security-level 50 ip address 172.16.1.12
```

```
255.255.255.0 ! interface Ethernet0/3 no nameif no
security-level no ip address ! interface Management0/0
no nameif no security-level no ip address ! !--- Output
is suppressed. !--- Permit inbound TFTP traffic. access-
list 100 extended permit udp any host 192.168.1.5 eq
tftp ! !--- Command to redirect the TFTP traffic
received on IP 192.168.1.5 !--- to IP 172.16.1.5. static
(DMZ,outside) 192.168.1.5 172.16.1.5 netmask
255.255.255.255 access-group 100 in interface outside
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
inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! !---
This command tells the device to !--- use the
"global_policy" policy-map on all interfaces. service-
policy global_policy global prompt hostname context
Cryptochecksum:4b2f54134e685d11b274ee159e5ed009 : end
ASA-AIP-CLI(config)#
```

確認

設定が正常に行われたことを確認するには、show service-policy コマンドを使用し、show service-policy inspect ftp コマンドを使用して出力を FTP 検査だけに制限します。

トラブルシューティング

問題： 設定の構文ははたらかないし、class-map 検査エラーは受け取られます

設定例に記載された構文が機能せず、次のようなエラーが表示されます。

```
ERROR: % class-map inspection_default not configured
```

解決策

この設定は、設定内にあるデフォルトの検査に依存しています。 設定内にデフォルトの検査がない場合は、次のコマンドを使用して再作成します。

1. class-map inspection_defaultmatch default-inspection-traffic
2. policy-map type inspect dns preset_dns_map parametersmessage-length maximum 512
3. policy-map global_policyclass inspection_defaultinspect dns preset_dns_mapinspect ftp inspect h323 h225inspect h323 rasinspect rshinspect rtspinspect esmtpinspect sqlnetinspect skinnyinspect sunrpcinspect xdmcpinspect sipinspect netbiosinspect tftp
4. service-policy global_policy global

警告： 以前に、別の問題を解決するために、デフォルトの検査が削除されている場合、デフォルトの検査が再度イネーブルになるとその問題が再発する可能性があります。 ユーザまたは管理者は、以前にトラブルシューティングの手順として、デフォルトの検査が削除されているかどうかを確認する必要があります。

ASA 全体で FTPS（FTP Over SSL）を実行できない

セキュリティ アプライアンスでは、TLS/SSL を使用した FTP (SFTP/FTPS) はサポートされていません。 FTP 接続は暗号化されるため、ファイアウォールによるパケットの復号化を可能にする方法はありません。 Cisco ASA をバージョン 8.2 以前と同じ構成にする場合は、『PIX/ASA：詳細についてはセキュリティ アプライアンス モデル FAQ。

関連情報

- ASA 5500 シリーズ適応型セキュリティ アプライアンス
- Cisco セキュリティ アプライアンス コマンド リファレンス
- PIX 500 シリーズ セキュリティ アプライアンス
- Cisco セキュリティ アドバイザリとセキュリティ通知
- テクニカルサポートとドキュメント - Cisco Systems