ASA 8.3 以降：FTP/TFTP サービスをイネーブルにする設定例

内容

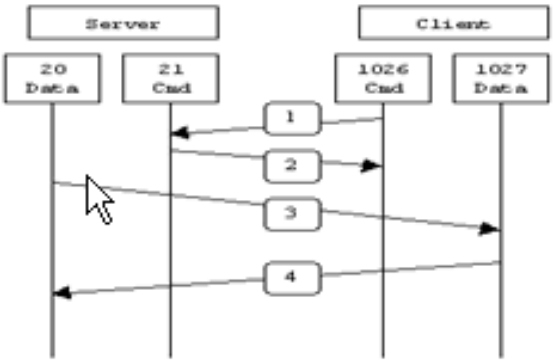
概要

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。

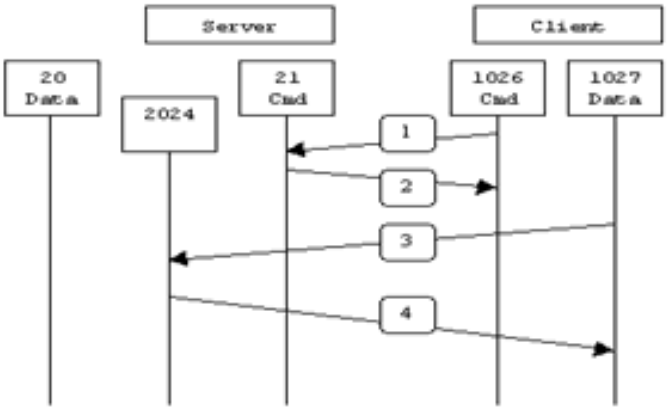
File Transfer Protocol (FTP)

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



Active FTP



Passive FTP

Active FTP :
command : client >1023 -> server 21
data : client >1023 <- server 20

Passive FTP :
command : client >1023 -> server 21
data : client >1023 -> server >1023

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、クライアントとサーバ間の接続は、どちらの方向でもクライアントによって開始されます。そのため、ファイアウォールでサーバからクライアントへの着信データ ポート接続がフィルタリングされるという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)。最初のポートはポート21上のサーバに接続します。しかし、次に**portコマンドを発行し**て、サーバがデータ· ポートに接続することを許可する代わりに、クライアントは**PASVコマンドを発行**します。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。

ソフトウェア バージョン 7.x が稼働する Cisco セキュリティ アプライアンスでのサイト間 IPSec VPN の設定方法の詳細については、『PIX/ASA 7.x : FTP/TFTP サービスをイネーブルにする設定例』を参照してください。

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 ネットワーク内に配置された FTP サーバの設定が完了している。

使用するコンポーネント

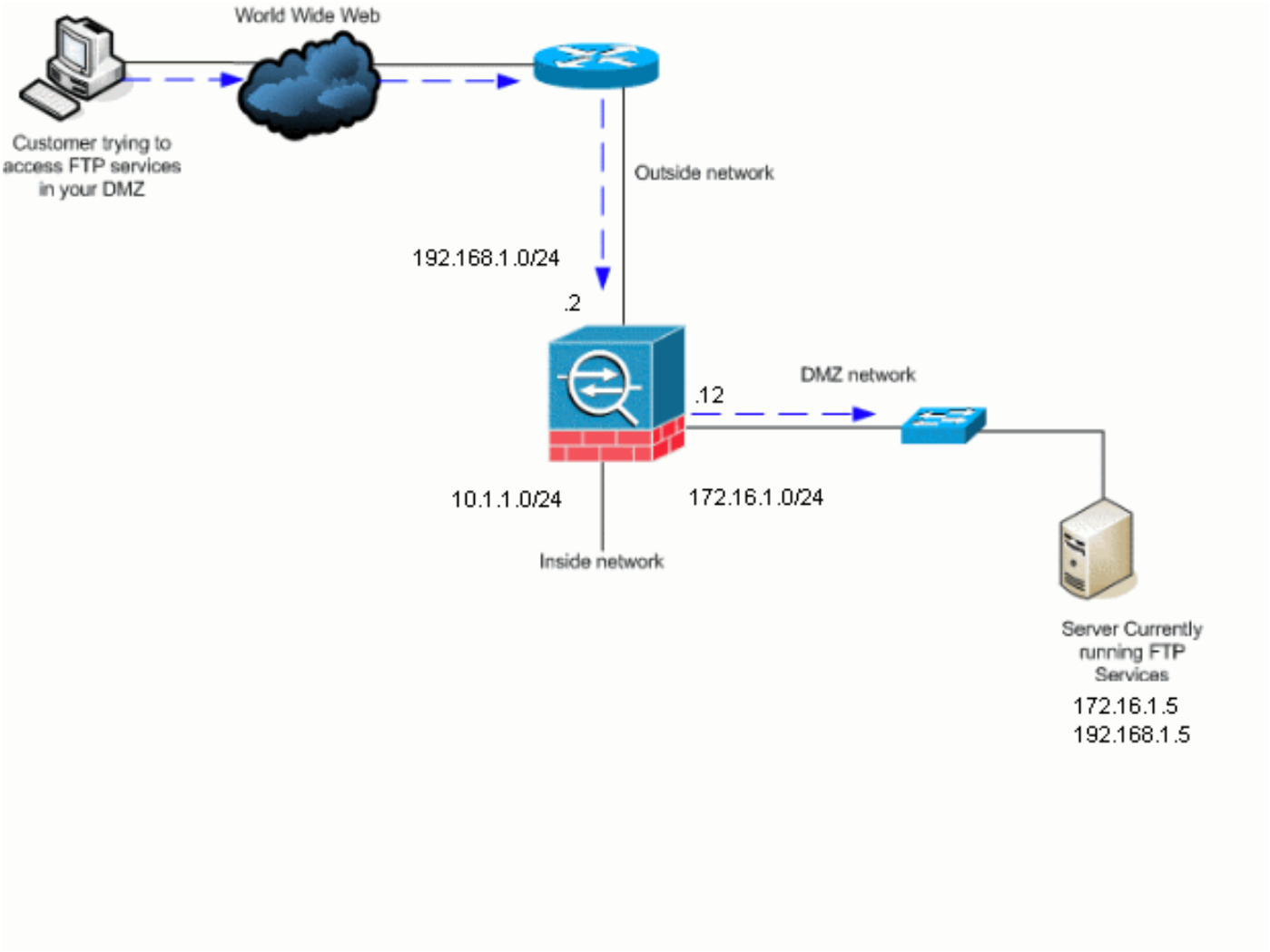
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- 8.4(1) 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。

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、ラボ環境で使用された RFC 1918 のアドレスです。

関連製品

この設定は、Cisco 適応型セキュリティ アプライアンス バージョン 8.3 以降にも適用できます。

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。

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 インスペクション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 インスペクションの実装は、次の処理で構成されています。

- トラフィックを識別する。
- トラフィックにインスペクションを適用する。
- インターフェイス上でインスペクションをアクティブにする。

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 アプライアンスのアプリケーション インスペクション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 インスペクション機能は、ネットワーク アドレス変換（NAT）と連動し、埋め込まれたアドレッシング情報の場所を識別できるようにします。

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 インスペクション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 インスペクション機能では、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 チャネルのインスペクションが必要になります。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 インスペクション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 アプライアンスは、アクティブとパッシブの FTP セッションの間での差異も認識します。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 インスペクションによって、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 インスペクションはデフォルトで有効になっています。

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、動的に接続および変換が作成されます。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 インスペクション 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インスペクションが適用されます。 デフォルトのアプリケーション インスペクション 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、非標準ポートにインスペクションを適用したり、デフォルトでは有効にならないインスペクション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無効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。**
   ```
   ASA(config)#policy-map global_policy
   ```
2. **class inspection_default コマンドを発行します。**
   ```
   ASA(config-pmap)#class inspection_default
   ```
3. **inspect FTP コマンドを発行します。**
   ```
   ASA(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 オプションをイネーブルにすると、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 RFCに厳密に準拠していないFTPクライアントに障害が発生す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(config)#show running-config

 ASA Version 8.4(1)
!
hostname ASA
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
!
!--- Object groups are created to define the hosts.
object network DMZ
host 172.16.1.5
```

```
object network DMZ-out
host 192.168.1.5
!--- Configure manual NAT nat (DMZ,outside) source
static DMZ DMZ-out
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(config)#
```

標準外 TCP ポートでの FTP プロトコル インスペクションの設定

次の設定を使用して、標準外 TCP ポートで FTP プロトコル インスペクションを設定できます（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 インスペクション 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インスペクションが適用されます。 デフォルトのアプリケーション インスペクション 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。そのため、グローバル ポリシーを変更する場合、たとえば、非標準ポートにインスペクションを適用したり、デフォルトでは有効にならないインスペクション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無効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。**
   ```
   ASA(config)#policy-map global_policy
   ```

2. **class inspection_default コマンドを発行します。**
   ```
   ASA(config-pmap)#class inspection_default
   ```

3. **inspect TFTP コマンドを発行します。**
   ```
   ASA(config-pmap-c)#inspect TFTP
   ```

設定例

デバイス名 1

```
ASA(config)#show running-config

 ASA Version 8.4(1)
!
hostname ASA
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
!
!--- Object groups are created to define the hosts.
object network DMZ
host 172.16.1.5
object network DMZ-out
host 192.168.1.5
!--- Configure manual NAT nat (DMZ,outside) source
static DMZ DMZ-out
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(config)#
```

確認

設定が正常に行われたことを検証するには、show service-policy コマンドを使用します。また、show service-policy inspect ftp コマンドを使用して、出力を FTP インスペクションだけに制限してください。

```
ASA#show service-policy inspect ftp
         Global Policy:
          Service-policy: global_policy
           Class-map: inspection_default
            Inspect: ftp, packet 0, drop 0, reste-drop 0
        ASA#
```

トラブルシュート

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- Cisco Adaptive Security Device Manager
- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- Requests for Comments (RFCs)
- テクニカル サポートとドキュメント – Cisco Systems