PIX/ASA 7.x：启用 FTP/TFTP 服务配置示例

目录

简介

本文档介绍网络外部的用户访问 DMZ 网络中的 FTP 和 TFTP 服务所需执行的步骤。

文件传输协议 (FTP)

有两种形式的 FTP：

- 主动模式
- 被动模式

在主动 FTP 模式下，客户端从一个随机的非特权端口 N (N>1023) 连接到 FTP 服务器的命令端口 (21)。然后，客户端开始监听端口 N+1，并将 FTP 命令 port N+1 发送到 FTP 服务器。接下来，服务器从其本地数据端口（端口 20）连接回客户端的指定数据端口。

在被动 FTP 模式下，客户端向服务器同时发起这两种连接，这将解决从服务器到客户端的数据端口传入连接被防火墙过滤掉的问题。当打开一个 FTP 连接时，客户端将在本地打开两个随机的非特权端口（N>1023 和 N+1）。第一个端口联系服务器的端口 21。然后，客户端发出 PASV 命令，而不是发出 port 命令并允许服务器连接回其数据端口。这样做的结果是服务器会打开一个随机的非特权

端口 P (P>1023)，并将 **port P** 命令发送回客户端。然后，客户端发起从端口 N+1 到服务器的端口 P 的连接来传输数据。如果安全设备上未配置 **inspection** 命令，内部用户发起的出站 FTP 只能以被动方式工作。此外，外部用户发起的访问 FTP 服务器的入站请求将被拒绝。

请参阅 ASA 8.3及以上版本：启用FTP/TFTP服务配置示例关于相同配置的更多信息使用ASDM用Cisco可适应安全工具(ASA)有版本8.3和以上的。

简单文件传输协议 (TFTP)

如 RFC 1350 中所述，TFTP 是一种用于在 TFTP 服务器与客户端之间读写文件的简单协议。TFTP 使用 UDP 端口 69。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 必需的接口之间存在基本通信。
- 已配置位于 DMZ 网络中的 FTP 服务器。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行 7.2(2) 软件映像的 ASA 5500 系列自适应安全设备
- 运行 FTP 服务的 Windows 2003 Server
- 运行 TFTP 服务的 Windows 2003 Server
- 位于网络外部的客户端 PC

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

网络图

本文档使用以下网络设置：

注意： 此配置中使用的 IP 编址方案在 Internet 上不可合法路由。这些地址是在实验室环境中使用的 RFC 1918 地址。

相关产品

此配置也适用于 PIX 安全设备 7.x。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

安全设备支持通过自适应安全算法功能进行应用程序检查。通过自适应安全算法所使用的状态应用程序检查，安全设备可跟踪穿过防火墙的每个连接，并确保这些连接有效。防火墙也通过状态检查来监控连接的状态，以便编译信息并放入状态表中。如果使用除了管理员定义的规则之外还使用状态表，则过滤决策将基于先前穿过防火墙的数据包所建立的上下文。实施应用程序检查包括下列操作：

- 标识流量。
- 对流量应用检查。
- 在接口上激活检查。

高级协议处理

FTP

某些应用程序要求由 Cisco 安全设备应用程序检查功能进行的特殊处理。此类应用程序通常将 IP 编址信息嵌入在用户数据包中，或者在动态分配的端口上打开辅助信道。应用程序检查功能可与网络地址转换 (NAT) 配合工作，帮助标识嵌入式编址信息的位置。

除了标识嵌入式编址信息外，应用程序检查功能还监控会话，以确定用于辅助信道的端口号。许多协议会打开辅助 TCP 或 UDP 端口以提高性能。某个已知端口上的初始会话用于协商动态分配的端口号。应用程序检查功能监控这些会话、标识动态端口分配，并允许在特定会话持续时间内通过这些端口进行数据交换。多媒体和 FTP 应用程序展示了这种行为。

由于 FTP 协议对每个 FTP 会话使用两个端口，因此该协议需要一些特殊处理。当激活 FTP 协议进行数据传输时，FTP 协议使用两个端口：使用端口 21 的控制信道和使用端口 20 的数据信道。通过控制信道发起 FTP 会话的用户将通过该信道发出所有数据请求。然后，FTP 服务器通过服务器端口 20 向用户计算机发起打开端口的请求。FTP 始终使用端口 20 进行数据信道通信。如果安全设备上尚未启用 FTP 检查，此请求将被丢弃，并且 FTP 会话不传输任何请求的数据。如果安全设备上启用了 FTP 检查，安全设备将监控控制信道，并尝试识别打开数据信道的请求。FTP 协议将数据信道端口规范嵌入在控制信道流量中，并要求安全设备检查控制信道中是否进行了数据端口更改。如果安全设备识别出某个请求，它将为会话生存期内持续的数据信道流量临时创建一个数据通路。通过这种方式，FTP 检查功能可监控控制信道、标识数据端口分配，并允许在会话持续时间内通过数据端口交换数据。

默认情况下，安全设备通过全局检查类映射检查端口 21 连接的 FTP 流量。安全设备还能识别出主动 FTP 会话与被动 FTP 会话之间的差别。如果 FTP 会话支持被动 FTP 数据传输，则安全设备可通过 **inspect ftp** 命令识别来自用户的数据端口请求并打开一个大于 1023 的新数据端口。

FTP 应用程序检查功能检查 FTP 会话并执行以下四个任务：

- 准备动态辅助数据连接
- 跟踪 FTP 命令响应顺序
- 生成审计线索
- 使用 NAT 转换嵌入式 IP 地址

FTP 应用程序检查准备辅助信道以进行 FTP 数据传输。响应文件上载、文件下载或目录列表事件时会分配信道，但必须预先协商这些信道。可通过 **PORT** 或 PASV (227) 命令协商端口。

TFTP

默认情况下 TFTP 检查功能已启用。

安全设备检查 TFTP 流量并动态地创建连接和转换（如果需要），以便允许在 TFTP 客户端与服务器之间传输文件。具体而言，检查引擎会检查 TFTP 读请求 (RRQ)、写请求 (WRQ) 和错误通知 (ERROR)。

在收到有效的 RRQ 或 WRQ 时会分配动态辅助信道和 PAT 转换（如果需要）。随后，TFTP 使用此辅助信道进行文件传输或错误通知。

只有 TFTP 服务器才能通过辅助信道发起流量，并且 TFTP 客户端与服务器之间最多只能存在一个不完整的辅助信道。服务器发出的错误通知会关闭辅助信道。

如果静态 PAT 用于重定向 TFTP 数据流，则必须启用 TFTP 检查。

配置基本的 FTP 应用程序检查

默认情况下，配置中包括一个与所有的默认应用程序检查流量匹配且对所有接口上的流量应用检查的策略（全局策略）。默认应用程序检查流量包括到每个协议的默认端口的流量。只能应用一个全局策略。因此，如果要改变全局策略（例如，对非标准端口应用检查，或者添加默认情况下未启用的检查），则需要编辑默认策略，或者禁用默认策略并应用新的策略。有关所有默认端口的列表，请参阅默认检查策略。

1. 发出 **policy-map global_policy** 命令。`ASAwAIP-CLI(config)#policy-map global_policy`
2. 发出 **class inspection_default** 命令。`ASAwAIP-CLI(config-pmap)#class inspection_default`
3. 发出 **inspect FTP** 命令。`ASAwAIP-CLI(config-pmap-c)#inspect FTP` 可以选择使用 **inspect FTP strict** 命令。此命令通过阻止 Web 浏览器在 FTP 请求中发送嵌入式命令，提高了受保护网络的安全性。在接口上启用 **strict** 选项后，FTP 检查功能将强制执行以下行为：必须先确认 FTP 命令，然后安全设备才允许新的命令。安全设备将断开发送嵌入式命令的连接。检查 **227** 和 PORT 命令，确保它们未出现在错误字符串中。**警告：** 使用 **strict** 选项可能会导致未严格遵循 FTP RFC 的 FTP 客户端出现故障。有关使用 **strict** 选项的详细信息，请参阅使用 strict 选项。

配置示例

设备名称 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)#
```

对非标准 TCP 端口配置 FTP 协议检查

使用下列配置行可以配置非标准 TCP 端口的 FTP 协议检查（将 XXXX 替换为新的端口号）：

```
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
```

配置基本的 TFTP 应用程序检查

默认情况下，配置中包括一个与所有的默认应用程序检查流量匹配且对所有接口上的流量应用检查的策略（全局策略）。默认应用程序检查流量包括到每个协议的默认端口的流量。只能应用一个全局策略。因此，如果要改变全局策略（例如，对非标准端口应用检查，或者添加默认情况下未启用的检查），则需要编辑默认策略，或者禁用默认策略并应用新的策略。有关所有默认端口的列表，请参阅默认检查策略。

1. 发出 policy-map global_policy 命令。`ASAwAIP-CLI(config)#policy-map global_policy`
2. 发出 class inspection_default 命令。`ASAwAIP-CLI(config-pmap)#class inspection_default`
3. 发出 inspect TFTP 命令。`ASAwAIP-CLI(config-pmap-c)#inspect TFTP`

配置示例

设备名称 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)#
```

验证

为了确保配置已成功实施，请使用 **show service-policy** 命令，并使用 show service-policy inspect ftp 命令限制输出仅为 FTP 检查。

故障排除

问题：配置中的语法无效，收到类映射检查错误

配置部分中提供的语法无效，并且收到如下错误：

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

解决方案

此配置依赖于配置中的默认检查。如果默认检查未包括在配置中，请使用以下命令重新创建它们：

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： 如果先前为了解决其他问题而删除了默认检查，当重新启用默认检查时，该问题可能会重现。您或管理员应该了解先前在故障排除过程中是否删除了默认检查。

无法通过 ASA 运行 FTPS（SSL 上的 FTP）

安全设备不支持使用 TLS/SSL 的 FTP (SFTP/FTPS)。FTP 连接是加密的，因此防火墙无法解密数据包。请参阅 PIX/ASA：安全设备常见问题。

相关信息

- ASA 5500 系列自适应安全设备
- Cisco 安全设备命令参考
- PIX 500 系列安全设备

- Cisco 安全建议和通知
- 技术支持和文档 - Cisco Systems