与FXP配置示例的ASA文件传输

目录

简介

本文描述如何通过CLI配置文件交换协议(FXP)在思科可适应安全工具(ASA)。

先决条件

要求

思科建议您有基础知识文件传输协议(FTP) (有源/无源模式)。

使用的组件

运行软件版本8.0及以后的本文档中的信息根据Cisco ASA。

> **注意**：此配置示例使用作为FXP服务器和运行FTP服务的两个Microsoft Windows工作站(3C守护程序)。他们也安排FXP启用。运行FXP客户端软件(FTP仓促)也使用的另一个Microsoft Windows工作站。

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。

背景信息

FXP允许您转接从一个FTP服务器的文件到另一个FTP服务器通过FXP客户端，不用需要取决于客户端互联网连接速度。使用FXP，最大转移速度仅取决于两个服务器之间的连接，比客户端连接通常快速。您能应用在一个高带宽服务器需求从另一个高带宽服务器的资源的方案的FXP，但是只有一个低带宽客户端例如远程工作的网络管理员有访问的权限在两个服务器的资源。

FXP工作作为FTP协议的分机，并且机制在FTP RFC 959的第5.2部分陈述。基本上， FXP客户端首次与FTP server1的一个控制连接，打开与FTP server2的另一个控制连接，然后修改服务器的连接属性，以便他们彼此指向这样转移发生直接地在两个服务器之间。

文件传输机制通过FXP

这是进程的概述：

1. 客户端打开与server1的一个控制连接在TCP端口21。

   客户端发送**pasv命令**对server1。

   Server1回应侦听的其IP地址和端口。

2. 客户端打开与server2的一个控制连接在TCP端口21。

   从server1接收到在端口命令的server2的客户端通过地址/端口。

   Server2响应为了通知**port命令**是成功的客户端。Server2在哪里当前知道发送数据。

3. 为了开始发射进程从server1到server2 ：

   客户端发送**STOR**命令对server2并且指示它存储日期接收。

   客户端发送**RETR命令**对server1并且指示它检索或传送文件。

4. 所有数据直接地从来源当前去目的地FTP服务器。两个服务器只在失败/成功的状态消息向客户端报告。

这是连接表如何出现：

```
TCP server2 192.168.1.10:21 client 172.16.1.10:50684, idle 0:00:04, bytes 694,
flags UIOB
TCP client 172.16.1.10:50685 server1 10.1.1.10:21, idle 0:00:04, bytes 1208,
flags UIOB
```

FTP检查和FXP

只有当FTP检查在ASA时，**禁用**文件传输通过ASA通过FXP是成功的。

当FXP客户端指定与那些**port命令的**FTP的客户端有所不同的IP地址和TCP端口时，一个不安全情况创建攻击者能执行端口扫描在互联网的一台主机从一个第三方FTP服务器的地方。这是因为FTP服务器被指示打开对端口的一连接在也许不是客户端产生的计算机。这呼叫**FTP跳动攻击**，并且FTP检查关闭连接，因为认为此安全侵害。

示例如下：

```
%ASA-6-302013: Built inbound TCP connection 24886 for client:172.16.1.10/49187
(172.16.1.10/49187) to server2:192.168.1.10/21 (192.168.1.10/21)
%ASA-6-302013: Built inbound TCP connection 24889 for client:172.16.1.10/49190
(172.16.1.10/49190) to server2:192.168.1.10/49159 (192.168.1.10/49159)
%ASA-6-302014: Teardown TCP connection 24889 for client:172.16.1.10/49190 to
server2:192.168.1.10/49159 duration 0:00:00 bytes 1078 TCP FINs
%ASA-4-406002: FTP port command different address: 172.16.1.10(10.1.1.10) to
192.168.1.10 on interface client
%ASA-6-302014: Teardown TCP connection 24886 for client:172.16.1.10/49187 to
server2:192.168.1.10/21 duration 0:00:00 bytes 649 Flow closed by inspection
```

配置

请使用在此部分描述为了配置在ASA的FXP的信息。

> **注意**：使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

通过 CLI 配置 ASA

完成这些步骤为了配置ASA ：

1. 禁用FTP检查：
   ```
   FXP-ASA(config)# policy-map global_policy
   FXP-ASA(config-pmap)#  class inspection_default
   FXP-ASA(config-pmap-c)# no inspect ftp
   ```
2. 配置访问列表为了允许FXP客户端和两个FTP服务器之间的通信：
   ```
   FXP-ASA(config)#access-list serv1 extended permit ip host 10.1.1.10 any
   FXP-ASA(config)#access-list serv1 extended permit ip any host 10.1.1.10
   FXP-ASA(config)#access-list serv2 extended permit ip host 192.168.1.10 any
   FXP-ASA(config)#access-list serv2 extended permit ip any host 192.168.1.10
   FXP-ASA(config)#access-list client extended permit ip host 172.16.1.10 any
   FXP-ASA(config)#access-list client extended permit ip any host 172.16.1.10
   ```
3. 运用在各自的接口的访问列表：
   ```
   FXP-ASA(config)#access-group serv1 in interface server1
   FXP-ASA(config)#access-group client in interface client
   FXP-ASA(config)#access-group serv2 in interface server2
   ```

验证

请使用在此部分描述为了验证的信息您的配置适当地工作。

文件传输进程

完成这些步骤为了验证在两个FTP服务器之间的成功的文件传输：

1. 连接对从FXP客户端机器的server1 ：

2. 连接对从FXP客户端机器的server2 ：

3. 拖放从server1窗口将转接的文件到server2窗口：

4. 验证文件传输是成功的：

故障排除

此部分提供您能使用为了排除故障您的配置两个不同的方案的捕获。

FTP检查已禁用方案

当FTP检查禁用时，详情参见FTP检查和本文的FXP部分，此数据出现在ASA客户端接口：

这是关于此数据的一些笔记：

- 客户端IP地址是**172.16.1.10**。
- Server1 IP地址是**10.1.1.10**。
- Server2 IP地址是**192.168.1.10**。

在本例中，名为**Kiwi_Syslogd.exe的**文件从server1转接到server2。

FTP检查

当FTP检查启用时，此数据出现在ASA客户端接口：

这是ASA丢弃捕获：

Port请求由FTP检查丢弃，因为包含与客户端IP地址和端口有所不同的IP地址和端口。随后，对服务器的控制连接由检查终止。