

原创

置顶

依韵 |

2018-05-28 16:44:30

7164

收藏10

版权


分类专栏:

计算机基础知识

文章标签:

windows防火墙

FTP服务器

计算机基础知识 专栏收录该内容

0 订阅

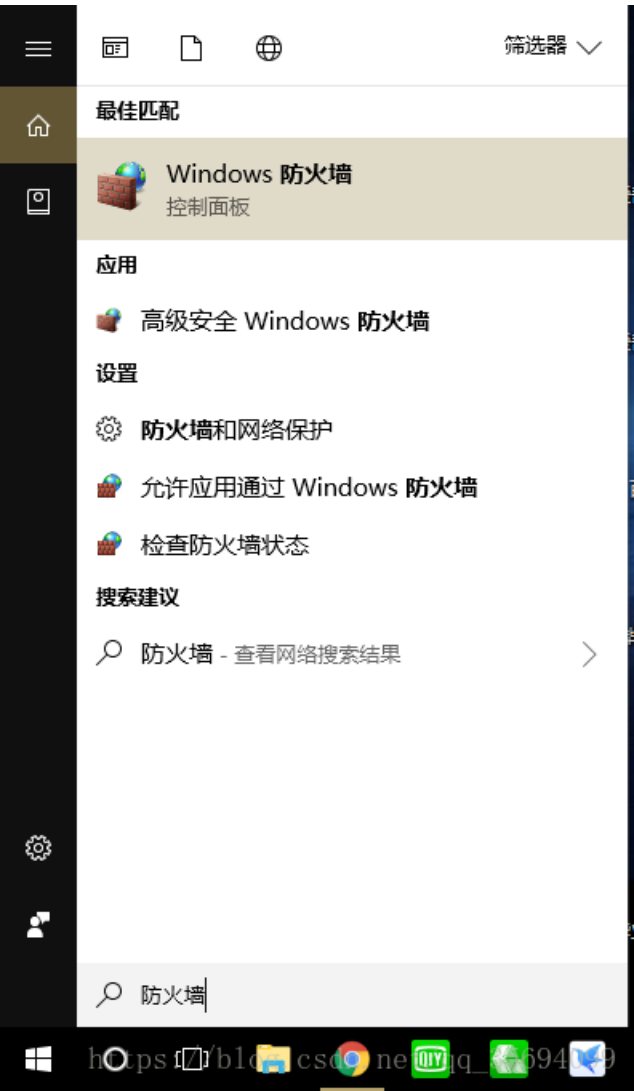
15 篇文章

订阅专栏

Windows防火墙的打开与关闭

1、在Windows10中打开 和关闭防火墙

我们点击**Windows10**系统下的**cortana**，并输入防火墙即可找到**Windows**防火墙。

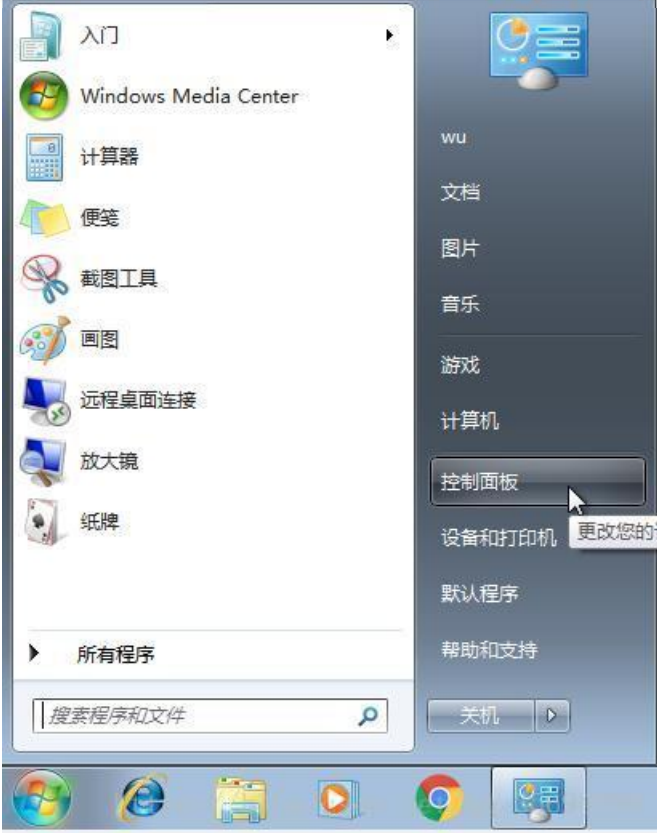


在下图所示的界面中我们可以对防火墙进行打开或者关闭的操作



https://blog.csdn.net/qq_35694099

2、在虚拟机的windows7系统中打开和关闭防火墙



之后在控制面板的页面中选择系统和安全



https://blog.csdn.net/qq_35694099

可以发现Windows防火墙的选项



https://blog.csdn.net/qq_35694099



依韵 I

关注

2

0

10



专栏目



windows防火墙对FTP服务器的影响

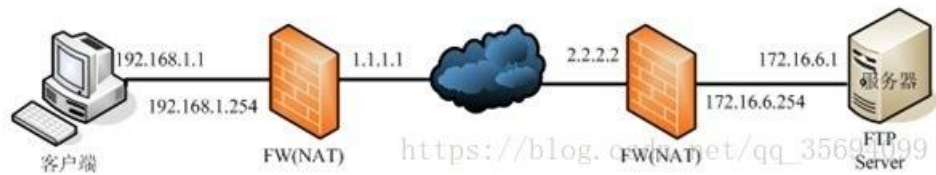
FTP 是常见的基于 TCP 的网络服务，它使用了两个TCP连接 来建立逻辑通信信道，即 控制连接 和 数据连接 。当客户端与服务器建立一个FTP会话时，使用TCP创建一个持久的 控制连接 以传递命令和应答。当发送文件和其它数据传输时，它们在独立的TCP 数据连接 上进行传递，这个连接根据需要创建和拆除。

更为复杂的是，FTP标准指定了创建 数据连接 的两种不同方法，即 正常（主动）数据连接 和 被动数据连接 。FTP的 控制连接 总是由 客户端 首先发起的， 主动数据连接 是由 客户端 发起的， 被动数据连接 是由 服务器端 发起的。

成功建立 控制连接 后，在进行主动连接时，客户端发送 PORT命令 ，其中内嵌了 地址和端口信息 ，以告知服务器进行连接，然后服务器打开 默认端口20 建立到 客户端已告知地址和端口 的数据连接。在进行被动连接时，客户机使用 PASV命令 告诉服务器等待客户机建立数据连接，服务器响应，告诉客户机为了数据传输它应该使用服务器上的什么端口（随机打开）。这种工作机制带来了一个严重的问题： 在FTP的命令（PORT或PASV）或对它们的回答中传递IP地址及端口号与网络分层机制严重冲突 ， 在FTP客户端与服务器的通信信道之间的网关设备（防火墙或路由器）上启用了NAT功能的情况下将出现连接性问题 。

防火墙对于像FTP这样的多端口连接的TCP应用，其影响是深远的，在复杂的网络环境中，更是由于设备、软件的多样性可能导致不可预知的问题。作为一名网络管理员，深入了解防火墙和FTP的工作原理及其在NAT环境下防火墙对FTP的影响，对于选择FTP服务软件及安装、部署、管理及维护FTP服务和实际工作中排除FTP应用故障是大有裨益的。本文就以一个在实际环境中比较常见的FTP部署和应用拓扑为例，来详细解读 防火墙（启用了NAT功能）对FTP 的影响。如有不当之处，敬请指正。

一、网络拓扑图



二、主动模式的连接分析

如本例中网络拓扑所示，IP为192.168.1.1客户端计算机打开一个可用的 TCP端口1025 ，经过其前端的 防火墙 进行 NAT转换成地址1.1.1.1和端口1025后建立到目标地址为2.2.2.2的21端口的连接 ，然后服务器前端的防火墙将此连接信息传递到服务器172.16.6.1的21端口，成功建立FTP控制连接。

服务器则经由这个已经建立的逻辑连接通道返回数据包，与客户端进行交互。接着，客户端发出 PORT指令 ，在指令中嵌入了 地址信息（IP:192.168.1.1, Port:1026） ，告知服务器用于数据连接，并打开端口1026，等待服务器连接。当承载PORT指令的数据包到达客户机前端的防火墙时，由于NAT的缘故，在成功创建NAT表项，改写数据包的IP和TCP端口信息后：

如果此时 防火墙 不能识别并检查此连接是FTP应用，便不能对 PORT指令 中嵌入的地址和端口信息进行改写， 则将此数据包通过先前已建立的控制连接通道传递到服务器后，服务器则打开20端口 ， 将建立到192.168.1.1的1026端口的数据连接 。

显然，此连接数据包要么被其前端的防火墙丢弃，要么在流入因特网后立刻被丢弃，永远无法到达客户端 。在这种情况下，客户端一直处在控制连接阶段发送含有PORT指令的数据包，以便建立数据连接；而服务器则在打开了20端口后，一直尝试建立到客户端的数据连接，但始终收不到应答。

直接的结果就是： 客户端成功连接了FTP服务器，却无法进行数据传输 。这里可能还包含一个隐藏的安全威胁：如果恰巧192.168.1.1对于服务器主机来

机，在这两台主机之间产生莫名的数据流。



依韵 |

关注

2

0

10



专栏目

服务器收到PORT指令后，打开20端口，建立到1.1.1.1上1026端口的连接，成功交互后，便能进行数据传输了。

三、被动模式的连接分析

控制连接建立后，客户端发出的 **PASV指令** 到达服务器，服务器则随机打开一个可用的TCP端口，并将地址和端口信息（IP:172.16.6.1，Port:50000）返回给客户端，告知客户端利用这些信息进行数据连接。当包含服务器地址信息的这个数据包到达其前端的防火墙时：

如果防火墙不能识别并检查此数据包的应用层数据， 无法判定它是**FTP的PASV指令**的返回包，并对其中嵌入的地址信息进行重写， 则当此数据包返回到客户端时，客户端将随机打开端口**3000**，以目的地址**172.16.6.1**、端口**50000**来进行数据连接，同理，此连接数据包永远不能到达服务器端。

这种情况下，客户端将一直尝试建立数据连接，却总是不能收到应答。这里可能包含的隐藏安全威胁，如前所述。

如果防火墙能对**FTP应用**进行审查和跟踪，并将返回包中嵌入的服务器地址信息进行重写，即转换成（**IP：2.2.2.2，Port：50000**），然后建立新的**NAT**表项，动态打开**50000**端口，等待连接。则此返回包到达客户端时，客户端将随机打开端口**3000**，以目的地址**2.2.2.2**、端口**50000**来新建连接，便能成功建立数据连接。

根据以上分析，为成功进行FTP数据传输， 主动模式下要求客户机前端的 防火墙在启用**NAT**后能对**FTP应用**进行审查和跟踪，识别并改写**PORT**指令中的客户端地址信息； 被动模式下则要求服务器前端的防火墙能改写服务器响应**PASV**指令后返回数据包中的服务器地址信息。

当然，为保险起见，为保证FTP应用的正常使用，建议两端的防火墙都需要支持 对**FTP进行识别和内容审查**。

四、网络防火墙与FTP

大多数网管设置防火墙的默认访问控制策略是：允许从内部到外部的一切流量，禁止从外部到内部的一切流量。

就FTP应用来说，为了简化防火墙策略的配置又兼顾安全策略要求，客户机选择被动模式进行数据连接较好，不需要对其前端的防火墙设置特别的访问控制策略，但要求服务器前端的防火墙能动态打开数据连接所需的随机端口；服务器端则选择主动连接较好，为允许客户端的访问，其前端防火墙的访问控制策略仅需要显式对外开放21端口即可，但需要客户机前端的防火墙能动态打开数据连接所需的端口。

从方便使用的角度考虑，既然提供FTP服务，就要配置好 服务器前端的防火墙，使其访问控制策略能支持两种模式下的FTP服务正常工作。

如果客户机前端的NAT设备为路由器，不是防火墙，并不能审查和跟踪FTP应用，从前面的分析可以推断出，主动模式下肯定存在连接性问题，需要以被动方式建立数据连接才能成功使用FTP服务。

如果 **FTP控制端口**非默认，而是 定制的**TCP端口**（比如**2121**），在这种情况下， 服务器前端的防火墙通过配置命令显式指示**FTP**的控制端口，便能进行审查和跟踪。 但客户机前端的防火墙即使能识别默认端口下的**FTP应用**，此时也会把控制端口非**21**的**FTP服务**当作一般的**TCP应用**对待，这种情形下，便不能改写主动模式下的客户端地址端口信息，导致服务器在建立数据连接时失败，但客户端使用被动连接模式能正常工作。

综上所述， 客户端使用被动方式连接**FTP服务器**是最恰当的，能最大限度地降低连接性问题。同时降低了对客户机前端防火墙备的要求，不需要像主动方式那样动态开放允许输入的随机端口，把可能的安全威胁推给了服务器端。这或许是微软的IE浏览器（资源管理器）默认设置使用被动方式的原因。如图表2所示。另外需要注意的， 在**Windows命令行**下，**FTP默认**是使用主动方式进行数据连接的。



五、主机防火墙与FTP

如果将FTP服务器架设在Windows Server 2003上，那么，在Windows Server 2003上安装并配置好FTP服务后，以客户端建立到这台FTP服务器的控制连接



依韵 |

关注

👍 2

💬 0

🌟 10



专栏目



依韵丨

码龄5年

🔒 暂无认证

35

10万+

171万+

30万+



原创

周排名

总排名

访问

等级

1811

44

120

55

220

积分

粉丝

获赞

评论

收藏

7





私信

关注

搜博文文章

🔍

- 热门文章
- 关于在Windows10下需要Administrators权限才能删除该文件问题的解决办法（亲测可用）

👁 95298
- 在Virtual Box中安装Windows7 64位虚拟机系统

👁 50661
- PING、ARP -a、ipconfig等网络测试命令的具体使用

👁 27444
- 通过windows的远程桌面功能，实现从本机访问虚拟机桌面

👁 22654
- 在安卓手机上安装FTP客户端应用，实现通过手机访问计算机FTP服务器。

👁 18319

- 分类专栏
- JAVA

3篇
- SQLite

8篇
- NYOJ刷题记录

1篇
- 算法

1篇
- 计算机基础知识

15篇
- JSP

4篇
- ▼

- 最新评论
- 关于在Windows10下需要Administrators...
goodnameisused: 那个Lenovo文件夹里有个LenovoInternetServiceFramework的转 ...
- PING、ARP -a、ipconfig等网络测试命令...
儒雅的烤地瓜: 🤔
- 在Virtual Box中安装Windows7 64位虚拟...
梭 哈: 为啥我这个选择完启动盘之后，就上面一行代码下面都是黑的，然后不动了🔥 ...
- 关于在Windows10下需要Administrators...
Jamieln: 整吐了 改个名结果删掉了
- 关于在Windows10下需要Administrators...
收买神的欢心: 我也是 删不了 你解决了👍

您愿意向朋友推荐“博客详情页”吗？











强烈不推荐

不推荐

一般般

推荐

强烈推荐

最新文章

JAVA吸收回车符

2019年 1篇 2018年 35篇
2017年 1篇

目录

Windows防火墙的打开与关闭

- 1、在Windows10中打开 和关闭防火墙
- 2、在虚拟机的windows7系统中打开...

windows防火墙对FTP服务器的影响

- 一、网络拓扑图
- 二、主动模式的连接分析
- 三、被动模式的连接分析
- 四、网络防火墙与FTP
- 五、主机防火墙与FTP



依韵 I

关注

👍 2

💬 0

★ 10



专栏目