

HCIE-Security 备考指南

文件过滤



HCIE 只是一个开始....

HCIE 仅是一个证书...懂得做人和处事比证书和技能更重要...

希望大家顺利通过 HCIE，取得更好的职业发展！

目 录

HCIE-Security 文件过滤需要掌握的知识点.....	1
文件过滤简介.....	1
文件过滤原理描述.....	1
使用限制和注意事项	3
应用场景.....	3
文件过滤全局配置.....	5
配置文件过滤.....	5
举例：配置文件过滤.....	8
配置的文件过滤没有生效.....	15
现象描述.....	15
可能原因.....	15
处理步骤.....	15
配置了文件过滤后影响了正常的文件传输.....	16
现象描述.....	17
可能原因.....	17
处理步骤.....	17
文件过滤 FAQ.....	18

HCIE-Security 文件过滤需要掌握的知识点

- 熟悉文件过滤技术原理以及应用

文件过滤简介

介绍文件过滤特性的定义和目的。

定义

文件过滤是一种根据文件类型对通过防火墙的文件进行过滤的安全机制。

目的

随着社会和网络技术的不断发展，公司机密信息和用户个人信息的泄露已经成为信息安全的核心问题之一。另外病毒常感染或附着在文件中，且病毒的反检测和渗透防火墙的能力越来越强。因此文件安全已经是人们越来越关注的问题。但传统的防火墙和 UTM 设备已经不能满足这些需求。

在此背景下，文件过滤技术应运而生。文件过滤能根据文件的类型对文件进行过滤。

机密信息和病毒往往存在于特定的文件类型中，例如机密信息一般保存在文档文件中，病毒信息一般附着在可执行文件中。因此文件过滤通过阻断特定类型文件的传输，可以降低机密信息泄露和内网感染病毒的风险。

如果管理员想进一步降低机密信息泄露的风险，可以将文件过滤与内容过滤功能结合使用。

如果管理员想进一步降低内网感染病毒的风险，可以将文件过滤与反病毒功能结合使用。

文件过滤原理描述

NGFW 能够识别通过自身传输的文件的类型，并且可以对特定类型的文件进行阻断或告警。

由[安全策略原理描述](#)可知，当通过 NGFW 的文件（流量）匹配了一条安全策略规则，规则的动作作为 **permit** 且引用了文件过滤配置文件时，此文件需要进行文件过滤检测。

1. NGFW 能够识别出承载文件的应用、文件传输方向、文件类型和文件扩展名。

- 承载文件的应用：文件是承载在应用协议上传输的，例如 HTTP、FTP、SMTP、POP3、NFS、SMB、IMAP。
 - 文件传输方向：包括上传和下载。
 - 文件类型：NGFW 能够识别文件真正的类型。例如：一个 Word 文档 file.doc 可以将文件名修改为 file.exe，但是它的文件类型仍然为 doc。
 - 文件扩展名：文件名称（包含压缩文件）的后缀。例如：file.doc 和 file.exe 中的 doc 和 exe 为文件扩展名。
2. 文件过滤全局配置定义了文件类型识别结果异常时的处理动作。如果文件类型识别结果正常则无需文件过滤全局配置处理。

文件类型识别结果有三种异常情况：

- 文件扩展名不匹配：文件类型与文件扩展名不一致。
 - 文件类型无法识别：无法识别出文件类型，且没有文件扩展名。
 - 文件损坏：由于文件被破坏而无法进行文件类型识别。
3. 如表 1 所示，NGFW 会根据文件类型识别的结果和文件过滤全局配置的处理结果来决定：是否进行文件过滤规则匹配以及匹配的条件是什么。

如果需要进行文件过滤规则匹配，则 NGFW 会将识别出的文件属性（应用、方向、文件类型、文件扩展名）与管理员定义的文件过滤配置文件的规则进行匹配。

如果文件的属性与规则的匹配条件全部匹配，则此文件成功匹配文件过滤配置文件的规则。如果其中有一个条件不匹配，则继续匹配下一条规则。以此类推，如果所有规则都不匹配，则 NGFW 会允许此文件传输。

如果文件成功匹配一条规则，NGFW 将会执行此规则的动作。如果动作为“阻断”，则 NGFW 会阻断此文件传输。如果动作为“告警”，则 NGFW 会允许此文件传输并记录日志。

表 1 文件类型识别、全局配置、文件过滤规则匹配间的关系

1、文件类型识别结果	2、文件过滤全局配置	3、文件过滤规则匹配
文件类型与文件扩展名一致	-	根据文件类型进行文件过滤规则匹配，匹配条件为“应用”、“文件类型”、“方向”。

表 1 文件类型识别、全局配置、文件过滤规则匹配间的关系		
1、文件类型识别结果	2、文件过滤全局配置	3、文件过滤规则匹配
文件类型与文件扩展名不一致	执行“文件扩展名不匹配时动作”。 <ul style="list-style-type: none"> 告警：允许文件传输并记录日志，然后进行文件过滤规则匹配。 阻断：阻断文件传输并记录日志。 允许：允许文件传输，然后进行文件过滤规则匹配。 	根据文件类型进行文件过滤规则匹配，匹配条件为“应用”、“文件类型”、“方向”。
无法识别出文件类型，但存在文件扩展名	-	根据文件扩展名进行文件过滤规则匹配，匹配条件为“应用”、“自定义扩展名”、“方向”。
无法识别出文件类型，且没有文件扩展名	执行“文件类型无法识别时动作”。 <ul style="list-style-type: none"> 告警：允许文件传输并记录日志。 阻断：阻断文件传输并记录日志。 允许：允许文件传输。 	-
文件损坏	执行“文件损坏时动作”。 <ul style="list-style-type: none"> 告警：允许文件传输并记录日志。 阻断：阻断文件传输并记录日志。 允许：允许文件传输。 	-

使用限制和注意事项

配置文件过滤前请先阅读使用限制和注意事项。

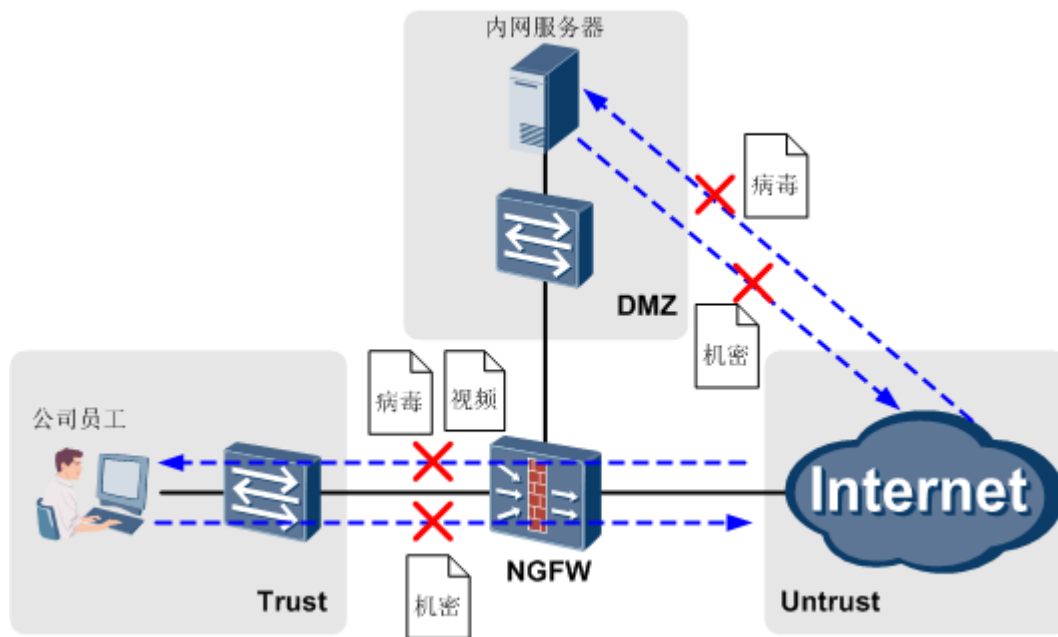
配置文件过滤前，请注意以下事项：

- 对于文件中嵌套的文件不进行文件类型过滤。
- 对于断点续传的文件不进行文件类型过滤。

应用场景

文件过滤功能可以降低机密信息泄露和病毒文件进入公司内部网络的风险，还可以阻止占用带宽和影响员工工作效率的文件传输。

图 1 文件过滤应用场景



文件过滤的应用场景如图 1 所示。管理员在 NGFW 上部署了文件过滤功能，可以实现如下安全保护效果：

- 降低机密信息泄露的风险。

机密信息一般保存在文档中，而且文档可以被压缩形成压缩文件。员工上传包含机密的文档到外网或者黑客从内网服务器窃取机密文档，都会导致公司机密或用户信息的泄露。

因此阻止内网用户上传文档文件和压缩文件到外网，以及阻止外网用户从内网服务器下载文档文件和压缩文件，可以大大降低机密信息泄露的风险。

- 降低病毒文件进入公司内部网络的风险。

病毒常常包含在可执行文件中，且病毒的反检测和渗透防火墙的能力越来越强。

因此阻止内网用户从外网下载可执行文件或阻断外网用户上传可执行文件到内网服务器，可以大大降低病毒进入内网的风险。

- 阻止占用带宽和影响员工工作效率的文件传输。

公司员工下载大量与工作无关的视频和图片文件，占用公司网络带宽，降低工作效率。

阻止内网用户从外网下载视频、图片和压缩文件，可以保证正常业务的带宽和员工的工作效率。

文件过滤全局配置

文件过滤全局配置是定义文件类型异常时的处理动作，通常采用默认值即可。

背景信息

文件过滤全局配置包括三种文件类型异常处理动作：

- 文件损坏时动作：文件损坏无法进行文件过滤、内容过滤和反病毒检测。
- 文件扩展名不匹配时动作：文件类型与文件扩展名不一致。如果动作为“允许”或“告警”，则按照文件类型进行文件过滤、内容过滤和反病毒检测。
- 文件类型无法识别时动作：无法识别出文件类型，且没有文件扩展名。不进行文件过滤、内容过滤和反病毒检测。

操作步骤

1. 选择“对象 > 安全配置文件 > 文件过滤”。
2. 选择“全局配置”页签。
3. 在参数后对应的下拉框中选择动作。
 - 告警：默认动作，允许文件传输并记录日志。
 - 阻断：阻断文件传输并记录日志。
 - 允许：不做任何处理，允许文件传输。

配置文件过滤

介绍了文件过滤特性的配置步骤。

背景信息

每条安全策略规则可以应用一个文件过滤配置文件，来阻断选定类型的文件的上传、下载，或者当检测到选定类型的文件时记录日志。

NGFW 中存在一个文件过滤的缺省配置文件，名称为 default。缺省配置文件中定义了 NGFW 支持的全部应用，全部文件类型的文件在上传方向上的响应动作均为告警。缺省配置文件不能被修改和删除。

<input type="checkbox"/> 名称	规则名称	应用	文件类型	自定义扩展名	方向	动作
<input type="checkbox"/> default	default	全部	全部		上传	告警

NGFW 支持创建自定义配置文件，您可以根据需要，对每类文件在上传或下载方向上应用不同的响应动作。

操作步骤

1. 选择“对象 > 安全配置文件 > 文件过滤”。
2. 单击“新建”。
3. 配置文件过滤配置文件的名称和描述。

参数	说明
名称	输入文件过滤配置文件的名称。名称必须是唯一的，不能有重复的名称。当配置安全策略时，名称会出现在“文件过滤”的参数选择列表中。
描述	输入文件过滤配置文件的描述信息。合理填写描述信息有助于管理员正确理解配置文件的功能，使配置文件变得方便选择、查找和维护。例如：阻断使用 FTP 协议下载 EXE 文件。

4. 配置文件过滤规则。
 - a. 在“文件过滤规则”中，单击“新建”。
 - b. 配置文件过滤规则的名称。

参数	说明
名称	输入文件过滤规则的名称。名称必须是唯一的，不能有重复的名称。

- c. 配置文件过滤规则的匹配条件。

设备会将识别出的文件属性与规则的匹配条件进行匹配，如果条件全部匹配，则执行规则的动作。如果其中有一个条件不匹配，则继续匹配下一条规则。如果所有规则都不匹配，则设备允许文件传输。

如果设备能够识别出文件类型，则文件过滤的匹配条件为“应用”、“文件类型”、“方向”。

如果设备不能够识别出文件类型，则文件过滤的匹配条件为“应用”、“自定义扩展名”、“方向”。

参数	说明
应用	选择想要进行文件过滤的应用。例如只想对通过 FTP 协议传输的文件的类型进行过滤，则这里选择 FTP。
文件类型	选择想要阻断或告警的文件类型。文件类型是设备能够识别的文件真正的类型。
自定义扩展名	输入自定义扩展名。自定义扩展名是文件类型的补充，当设备无法识别出文件类型时，将根据自定义扩展名进行文件过滤。
方向	选择想要检测的文件传输方向。 <ul style="list-style-type: none"> 上传：用户将文件从源地址发送到目的地址 下载：用户将文件从目的地址接收到源地址 双向：上传和下载



窍门：

管理员应该首先明确需要对哪些类型的文件进行过滤。然后在“文件类型”的下拉框中选择设备能够支持的文件类型。最后在“自定义扩展名”中填写剩余的文件类型。

例如：管理员明确需要对 exe、doc 和 flash 文件进行过滤。他在“文件类型”的下拉框中发现了 EXE 和 DOC 但没有发现 FLV，因此他选中了 EXE 和 DOC 两项并且在“自定义扩展名”中填写了“FLV”。

d. 配置文件过滤规则的动作。



说明：

- 由于 IMAP 与 NFS 协议不支持阻断动作，因此当“应用”选择“NFS”或“SMB”且“动作”选择“阻断”时，设备将执行告警动作。
- 当“应用”选择“SMTP”或“POP3”且“动作”选择“阻断”时，设备将执行删除附件的动作。

参数	说明
动作	选择当文件匹配全部条件时设备执行的动作。 <ul style="list-style-type: none"> 阻断：默认动作，阻断文件传输并记录日志。 告警：允许文件传输并记录日志。

e. 单击“确定”。

f. 反复执行步骤 [4.a-4.e](#)，可以新建多个文件过滤规则。

5. 单击“确定”，完成文件过滤配置文件的配置。

6. 在安全策略中引用文件过滤配置文件。

7. 单击界面右上角的“提交”，提交配置文件进行编译。

创建或修改安全配置文件后，配置内容不会立即生效，需要单击界面右上角的“提交”来激活。因为激活过程所需时间较长，建议您完成所有对安全配置文件的操作后再统一进行提交。

后续处理

查看或解除安全策略与配置文件的引用关系。

1. 在配置文件的列表界面单击“引用计数”下的“查看”，可以看到配置文件被哪些安全策略引用。
2. 选中安全策略后，单击“解除”，可以解除安全策略与此配置文件的引用关系。

单击“解除所有”，在弹出的对话框中单击“确定”，解除所有安全策略对此配置文件的引用。

举例：配置文件过滤

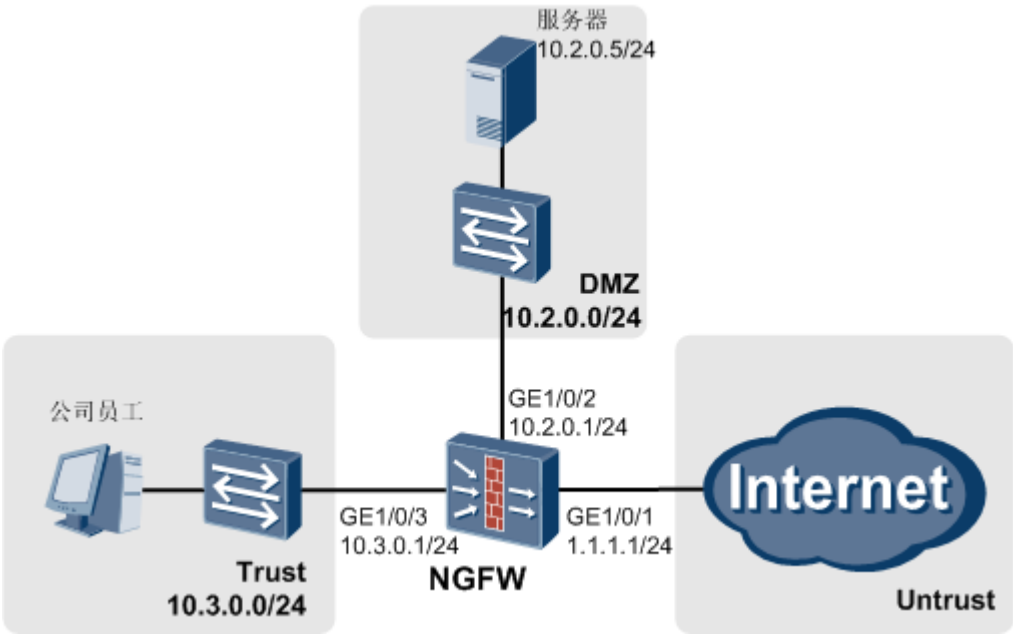
在企业网关配置文件过滤后，可以降低内部网络感染病毒的风险，还可以防止员工将公司机密文件泄露到互联网。

组网需求

如图1所示，某公司在网络边界处部署了 NGFW 作为安全网关。公司希望在保证网络能够正常使用的同时实现以下需求：

- 为了防止公司机密文件的泄露，禁止员工上传常见文档文件、开发文件（C、CPP、JAVA）以及压缩文件到内网服务器和 Internet。
- 为了降低病毒进入公司内部的风险，禁止员工从 Internet 下载可执行文件以及 Internet 用户上传可执行文件到内网服务器。
- 为了保证员工的工作效率，禁止员工从 Internet 下载视频类文件。

图 1 文件过滤组网图



数据规划

说明：

本举例的用户已经存在于 NGFW 中，并且已经完成了认证的配置。


项目	数据	说明
policy_sec_user1	<ul style="list-style-type: none">名称：policy_sec_user1源安全区域：trust目的安全区域：untrust用户：user动作：允许文件过滤：profile_file_user1	安全策略“policy_sec_user1”的作用是允许公司员工访问 Internet，引用文件过滤配置文件“profile_file_user1”可以禁止员工上传常见文档文件、开发文件和压缩文件到 Internet 以及禁止员工从 Internet 下载可执行文件和视频文件。
policy_sec_user2	<ul style="list-style-type: none">名称：policy_sec_user2源安全区域：trust目的安全区域：dmz目的地址/地区：10.2.0.5/24用户：user动作：允许文件过滤：profile_file_user2	安全策略“policy_sec_user2”的作用是允许公司员工访问内网服务器，引用文件过滤配置文件“profile_file_user2”可以禁止员工上传常见文档文件、开发文件以及压缩文件到内网服务器。
policy_sec_internet	<ul style="list-style-type: none">名称：policy_sec_internet源安全区域：untrust目的安全区域：dmz目的地址/地区：10.2.0.5/24动作：允许文件过滤：profile_file_internet	安全策略“policy_sec_internet”的作用是允许 Internet 用户访问内网服务器，引用文件过滤配置文件“profile_file_internet”可以禁止 Internet 用户上传可执行文件到内网服务器。
profile_file_user1	<ul style="list-style-type: none">名称：rule1	文件过滤配置文件“profile_file_user1”的规则

项目	数据	说明
	<ul style="list-style-type: none"> 文件类型：文档文件、压缩文件、代码文件 方向：上传 动作：阻断 	“rule1”的作用是禁止上传常见文档文件、开发文件以及压缩文件。
	<ul style="list-style-type: none"> 名称：rule2 文件类型：可执行文件、音视频文件 方向：下载 动作：阻断 	文件过滤配置文件“profile_file_user1”的规则“rule2”的作用是禁止下载可执行文件、视频和音频文件。
profile_file_user2	<ul style="list-style-type: none"> 名称：rule1 文件类型：文档文件、压缩文件、代码文件 方向：上传 动作：阻断 	文件过滤配置文件“profile_file_user2”的规则“rule1”的作用是禁止上传常见文档文件、开发文件以及压缩文件。
profile_file_internet	<ul style="list-style-type: none"> 名称：rule1 文件类型：可执行文件 方向：上传 动作：阻断 	文件过滤配置文件“profile_file_internet”的规则“rule1”的作用是禁止上传可执行文件。

配置思路

1. 配置接口 IP 地址和安全区域，完成网络基本参数配置。
2. 新建文件过滤配置文件。
3. 配置安全策略，保证网络可达的同时引用文件过滤配置文件，实现文件过滤。

操作步骤

1. 配置接口 IP 地址和安全区域，完成网络基本参数配置。
 - a. 选择“网络 > 接口”。
 - b. 单击 GE1/0/1 对应的 ，按如下参数配置。

IP 地址	1.1.1.1
网络掩码	255.255.255.0
安全区域	untrust

- c. 单击“应用”。
- d. 参考上述步骤按如下参数配置 GE1/0/2 接口。

IP 地址	10.2.0.1
网络掩码	255.255.255.0
安全区域	dmz

- e. 参考上述步骤按如下参数配置 GE1/0/3 接口。

IP 地址	10.3.0.1
网络掩码	255.255.255.0
安全区域	trust

2. 新建文件过滤配置文件。

- a. 选择“对象 > 安全配置文件 > 文件过滤”。
- b. 单击“新建”。
- c. 按如下参数新建文件过滤配置文件 profile_file_user1。

名称	profile_file_user1
文件过滤规则	
rule1	<ul style="list-style-type: none"> 名称: rule1 文件类型: 文档文件、压缩文件、代码文件 方向: 上传 动作: 阻断
rule2	<ul style="list-style-type: none"> 名称: rule2 文件类型: 可执行文件、音视频文件 方向: 下载 动作: 阻断

- d. 单击“确定”。
- e. 参考上述步骤按如下参数新建 profile_file_user2。

名称	profile_file_user2
文件过滤规则	
rule1	<ul style="list-style-type: none"> 名称: rule1 文件类型: 文档文件、压缩文件、代码文件 方向: 上传 动作: 阻断

- f. 参考上述步骤按如下参数新建 profile_file_internet。

名称	profile_file_internet
文件过滤规则	

rule1	<ul style="list-style-type: none"> • 名称: rule1 • 文件类型: 可执行文件 • 方向: 上传 • 动作: 阻断
--------------	--

3. 配置安全策略并引用配置文件。

- a. 选择“策略 > 安全策略 > 安全策略”。
- b. 单击“新建”。
- c. 按照如下参数配置安全策略 policy_sec_user1。

名称	policy_sec_user1
描述	允许公司员工访问 Internet
源安全区域	trust
目的安全区域	untrust
用户	/default/user
动作	允许
文件过滤	profile_file_user1

- d. 单击“确定”。
- e. 参考上述步骤按如下参数配置 policy_sec_user2。

名称	policy_sec_user2
描述	允许公司员工访问内网服务器
源安全区域	trust
目的安全区域	dmz
目的地址/地区	10.2.0.5/24
用户	/default/user
动作	允许
文件过滤	profile_file_user2

- f. 参考上述步骤按如下参数配置 policy_sec_internet。

名称	policy_sec_internet
描述	允许 Internet 用户访问内网服务器
源安全区域	untrust
目的安全区域	dmz
目的地址/地区	10.2.0.5/24

动作	允许
文件过滤	profile_file_internet

- 单击界面右上角的“提交”，提交安全配置文件进行编译。

结果验证

- 公司员工在内网的 PC 上能够正常访问 Internet 和内网服务器，但是上传文档文件、压缩文件、代码文件失败，从 Internet 下载可执行文件和视频文件失败。这表明 policy_sec_user1 和 policy_sec_user2 配置成功。
- 在 Internet 的 PC 上能够正常访问内网服务器，但是不能上传可执行文件到内网服务器。这表明 policy_sec_internet 配置成功。
- 如果想查看文件阻断时的日志详细信息，可以查看“内容日志”。方法如下：
 - 选择“监控 > 日志 > 内容日志”。
 - 单击“高级查询”，选择“类型”为“文件过滤”。
 - 单击“查询”，可以看到文件过滤功能的日志。

配置脚本

```
#
profile type file-block name profile_file_user1
rule name rule1
file-type pre-defined name DOC PPT XLS MSOFFICE DOCX PPTX XLSX PDF VSD MPP
file-type pre-defined name ODS ODT ODP EML UOF RAR TAR ZIP GZIP CAB
file-type pre-defined name BZ2 C CPP JAVA
application all
direction upload
action block
rule name rule2
file-type pre-defined name EXE MSI RPM OCX A ELF DLL PE MDI MOV
file-type pre-defined name MPEG AVI RMVB ASF SWF MP3 MP4 MIDI
application all
direction download
action block
profile type file-block name profile_file_user2
rule name rule1
file-type pre-defined name DOC PPT XLS MSOFFICE DOCX PPTX XLSX PDF VSD MPP
file-type pre-defined name ODS ODT ODP EML UOF RAR TAR ZIP GZIP CAB
```

```

file-type pre-defined name BZ2 C CPP JAVA
application all
direction upload
action block
profile type file-block name profile_file_internet
rule name rule1
file-type pre-defined name EXE MSI RPM OCX A ELF DLL PE
application all
direction upload
action block
#
interface GigabitEthernet1/0/1
ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/2
ip address 10.2.0.1 255.255.255.0
#
interface GigabitEthernet1/0/3
ip address 10.3.0.1 255.255.255.0
#
firewall zone trust
add interface GigabitEthernet1/0/3
#
firewall zone dmz
add interface GigabitEthernet1/0/2
#
firewall zone untrust
add interface GigabitEthernet1/0/1
#
security-policy
rule name policy_sec_user1
source-zone trust
destination-zone untrust
user /default/user
profile file-block profile_file_user1
action permit
rule name policy_sec_user2
source-zone trust
destination-zone dmz
destination-address 10.2.0.0 24
user /default/user
profile file-block profile_file_user2

```



```
action permit
rule name policy_sec_internet
  source-zone untrust
  destination-zone dmz
  destination-address 10.2.0.0 24
  profile file-block profile_file_internet
  action permit
```

配置的文件过滤没有生效

配置文件过滤后，某些应该被过滤掉的文件类型仍然能正常传输。

现象描述

NGFW 上配置了文件过滤功能，想要阻断特定类型的文件在安全区域间的传输。但是当管理员进行测试的时候发现，应该被阻断的文件类型仍然能够正常的传输。

可能原因

原因一：流量没有匹配正确的安全策略。

原因二：安全策略没有或引用了错误的文件过滤配置文件。

原因三：文件过滤规则的匹配条件配置错误。

原因四：文件过滤规则的“动作”为“告警”。

处理步骤

1. 原因一：流量没有匹配正确的安全策略。
 - a. 选择“监控 > 日志 > 策略命中日志”。
 - b. 单击右上方的“高级查询”后，输入“源用户”和“应用”。
 - 源用户：管理员进行测试时使用的用户账号的名称，例如“User0001”。
 - 应用：管理员进行测试时使用的协议或者应用程序名称。
 - c. 单击“查询”。
 - d. 在显示的安全策略日志中，查看管理员测试时的流量是否匹配了正确的安全策略。

- 如果没有匹配正确的安全策略，则选择“策略 > 安全策略 > 安全策略”，调整安全策略的顺序或参数。
- 如果确定匹配了正确的安全策略，则执行 2。

2. 原因二：安全策略没有或引用了错误的文件过滤配置文件。

- a. 单击 1 中查询到的安全策略的名称，在“修改安全策略”界面可以看到安全策略引用的“文件过滤”配置文件。
 - 如果安全策略没有引用或者引用的不是正确的“文件过滤”配置文件，则选择在配置规划时此安全策略计划引用的“文件过滤”配置文件。
 - 如果确定匹配了正确的安全策略，则执行 3。

3. 原因三：文件过滤配置文件的匹配条件配置错误。

- a. 单击“文件过滤”右侧的“配置”。
- b. 在“修改文件过滤配置文件”界面查看各文件过滤规则的条件是否正确。

查看各个规则“应用”、“文件类型”、“自定义扩展名”、“方向”是否能够成功匹配所有想要阻断的文件。

- 如果文件过滤规则的条件配置不正确，则修改文件过滤规则。
- 如果文件过滤规则的条件配置正确，则执行 4。

4. 原因四：文件过滤规则的“动作”为“告警”。

- a. 在“修改文件过滤配置文件”界面查看各文件过滤规则的动作。
 - 如果“动作”为“告警”，且与配置规划时计划的一致，则说明文件能够传输是正常的情况。
 - 如果“动作”为“告警”，但配置规划时计划的“动作”为“阻断”，则需要修改文件过滤规则的动作。

配置了文件过滤后影响了正常的文件传输

配置了文件过滤后，正常的上传和下载操作不能进行。

现象描述

NGFW 上配置了文件过滤功能，想要阻断特定类型的文件在安全区域间的传输。但是内网用户在使用时发现无法上传或下载本来应该能够正常传输的文件。

可能原因

原因一：流量没有匹配正确的安全策略。

原因二：流量被其他内容安全功能阻断。

原因三：文件过滤配置文件配置错误。

处理步骤

1. 原因一：流量没有匹配正确的安全策略。

- a. 选择“监控 > 日志 > 策略命中日志”。
- b. 单击右上方的“高级查询”后，输入“源用户”和“应用”。
 - 源用户：内网用户上传或下载时使用的用户账号的名称，例如“User0001”。
 - 应用：内网用户上传或下载时使用的协议或者应用程序名称。
- c. 单击“查询”。
- d. 在显示的安全策略日志中，查看内网用户上传或下载时的流量是否匹配了正确的安全策略。
 - 如果没有匹配正确的安全策略，则选择“策略 > 安全策略 > 安全策略”，调整安全策略的顺序或参数。
 - 如果确定匹配了正确的安全策略，则执行 [2](#)。

2. 原因二：流量被其他内容安全功能阻断。

- a. 单击 [1](#) 中查询到的安全策略的名称，在“修改安全策略”界面可以看到安全策略引用的配置文件。
- b. 根据引用的安全配置文件，分别查看不同的日志。
 - 反病毒、入侵防御：选择“监控 > 日志 > 威胁日志”。
 - URL 过滤：选择“监控 > 日志 > URL 日志”。

- 文件过滤、内容过滤、应用行为控制：选择“监控 > 日志 > 内容日志”。
- c. 在相应的日志界面，单击右上方的“高级查询”后，输入“安全策略”的名称。
- d. 单击“查询”，在显示的日志中查看“动作”为“阻断”的日志。
- 如果流量被文件过滤配置文件阻断，则执行 [3](#)。
 - 如果流量被其他配置文件阻断，则查看相关配置文件判断此流量是否确实需要被阻断。
 - 如果是，则结束故障诊断。
 - 如果不是，则修改相关配置文件的参数。
3. 原因三：文件过滤配置文件配置错误。
- a. 单击 [2](#) 中查询到的文件过滤配置文件的名称，在“修改文件过滤配置文件”界面查看文件过滤规则。
- b. 调整文件过滤规则的参数，保证文件过滤规则的条件不匹配正常的文件传输条件。

文件过滤 FAQ

文件过滤特性常见疑问的回答。

压缩文件中的文件类型是否能进行文件过滤？

NGFW 只支持文件类型为 TAR、ZIP 和 GZIP 压缩文件中的文件类型进行文件过滤。

加密文件是否能进行文件过滤？

NGFW 只支持文件类型为 DOC_ENC、PPT_ENC、XLS_ENC、OPC_ENC、ZIP_ENC、RAR_ENC、7ZIP_ENC 和 PDF_ENC 的加密文件进行文件过滤。