

# HCIE-Security 备考指南

## 内容过滤



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 内容过滤需要掌握的知识点.....	1
内容过滤简介.....	1
内容过滤原理描述.....	1
内容过滤应用场景.....	4
使用限制和注意事项.....	6
配置关键字组.....	6
配置内容过滤.....	8
举例：配置内容过滤.....	11
配置的内容过滤没有生效.....	22
现象描述.....	22
可能原因.....	22
处理步骤.....	23
配置了内容过滤后影响了正常内容的传输.....	24
现象描述.....	25
可能原因.....	25
处理步骤.....	25
内容过滤 FAQ.....	27
HCIE-Security 模拟面试问题及面试建议.....	27

## HCIE-Security 内容过滤需要掌握的知识点

- 熟悉内容过滤关键技术
- 掌握内容过滤技术的应用

### 内容过滤简介

介绍内容过滤特性的定义和目的。

#### 定义

内容过滤是一种对通过防火墙的文件或应用的内容进行过滤的安全机制。

#### 目的

随着互联网时代的发展，公司员工办公时越来越多的需要使用 Internet。比如员工需要通过 Internet 浏览网页、搜索信息、收发邮件、发送帖子和微博等。

员工在使用 Internet 的过程中可能会产生以下问题：

- 员工上传或发布公司的机密信息到 Internet，导致公司机密泄露。
- 员工浏览、发布、传播违规信息，对公司造成不好的影响甚至带来法律风险。
- 员工浏览和搜索与工作无关的内容，降低工作效率。

因此越来越多的公司希望拥有一台设备，既能保证公司员工正常访问 Internet，又能对员工接收和发送的信息内容进行过滤。

NGFW 的内容过滤功能可以满足这一需求，它对通过防火墙的包含特定内容的文件或应用进行过滤，主要作用如下：

- 阻止机密信息的传播，降低公司机密泄露的风险。
- 降低因员工浏览、发布、传播敏感信息而给公司带来的法律风险。
- 阻止员工浏览和搜索与工作无关的内容，保证工作效率。

### 内容过滤原理描述

通过深度识别流量中包含的内容，设备可以对包含特定关键字的流量进行阻断或告警。

## 内容过滤

内容过滤包括文件内容过滤和应用内容过滤。

文件内容过滤是对用户上传和下载的文件内容中包含的关键字进行过滤。管理员可以控制对哪些应用传输的文件以及哪种类型的文件进行文件内容过滤。

应用内容过滤是对应用协议中包含的关键字进行过滤。针对不同应用，设备过滤的内容不同，具体如表1所示。

表 1 应用内容过滤		
应用		过滤的内容
协议	HTTP	<ul style="list-style-type: none"> <li>上传方向： <ul style="list-style-type: none"> <li>用户发布微博的内容</li> <li>用户发帖的内容</li> <li>用户搜索输入的内容</li> <li>用户提交信息的内容（例如网络注册用户时提交的申请）</li> <li>上传文件的名称</li> </ul> </li> <li>下载方向： <ul style="list-style-type: none"> <li>用户浏览网页的内容</li> <li>使用 HTTP 协议下载文件的名称</li> </ul> </li> </ul>
	FTP	上传和下载文件的名称。
	SMTP	发送的邮件的标题、正文和附件名称。
	POP3	接收的邮件的标题、正文和附件名称。
	IMAP	接收的邮件的标题、正文和附件名称。
	RTMPT	通过 RTMPT 协议传输的文件的名称。
	FLASH	FLASH 文件的名称。
文件共享		共享文件的名称。
网页邮件		网页邮件的标题、正文和附件名称。

## 关键字

关键字是内容过滤时设备需要识别的内容，如果在文件或应用中识别出关键字，设备会对此文件或应用执行响应动作。关键字通常为机密信息（公司商业机密、用户个人信息的报告）或违规信息（色情、暴力、敏感或公司规定的违规信息等）。

关键字包括预定义关键字和自定义关键字。

- 预定义关键字是系统默认存在的可以识别的关键字，包括：银行卡号、信用卡号、社会安全号、身份证号、机密关键字（包括“秘密”、“机密”、“绝密”）。
- 自定义关键字是管理员自定义的需要识别的关键字，有文本和正则表达式两种定义方式。
  - 文本方式是使用文本的方式表示需要识别的关键字，例如管理员想要识别关键字“机密文件”，只需要自定义文本方式的关键字“机密文件”即可。文本方式配置简单，匹配精确。
  - 正则表达式方式是使用正则表达式的方式表示需要识别的关键字。与文本方式不同的是一个正则表达式可以表示多个关键字。例如正则表达式“abc.de”中的“.”可以匹配任意单个字符，所以“abc.de”可以表示“abcxde”、“abcyde”、“abc8de”等等。

正则表达式方式匹配更加灵活和高效，但配置需要遵循正则表达式规则。正则表达式规则如[表 2](#)所示。

表 2 正则表达式规则	
字符	说明
.	匹配任意单个字符。例如 <b>abc.de</b> 可以匹配 <b>abcade</b> 、 <b>abcyde</b> 、 <b>abc8de</b> 等等。 <b>说明：</b> 正则表达式不能以.结尾。
()	标记一个子表达式的开始和结束位置。
*	匹配前面的字符或表达式零次或多次。例如 <b>zo*</b> 可以匹配 <b>z</b> 、 <b>zo</b> 、 <b>zoo</b> 、 <b>zooo</b> 等等。
+	匹配前面的字符或表达式一次或多次。例如 <b>zo+</b> 可以匹配 <b>zo</b> 、 <b>zoo</b> ，但不可以匹配 <b>z</b> 。
	等同于或。例如 <b>z food</b> 可以匹配 <b>z</b> 或 <b>food</b> 。 <b>(z f)ood</b> 则匹配 <b>zood</b> 或 <b>food</b> 。
[]	匹配所包含的任意一个字符。例如 <b>[abc]</b> 可以匹配 <b>a</b> 、 <b>b</b> 、 <b>c</b> 中的任意一个字符。
-	用于创建范围表达式。例如 <b>[c-z]</b> 可以匹配 <b>c</b> 和 <b>z</b> 之间的任意一个字符，包括 <b>c</b> 和 <b>z</b> 。
{n}	<b>n</b> 是一个小于等于 20 的非负整数。匹配前面的字符 <b>n</b> 次。例如， <b>o{2}</b> 不能匹配 <b>Bob</b> 中的 <b>o</b> ，但是能匹配 <b>food</b> 中的两个 <b>o</b> 。
\	要对上述任一特殊字符执行字面匹配，必须通过在这些字符前面加上\（反斜杠），对这些字符进行转义。例如\ <b>.</b> 、\ <b>(和\)</b> 。
\d	匹配一个数字字符。等价于 <b>[0-9]</b> 。
\w	匹配数字、字母和下划线。

## 响应动作

当设备在内容过滤检测时识别出关键字，设备会执行响应动作，如[表 3](#)所示。

表 3 响应动作	
动作	说明
告警	识别出关键字后，记录日志但不阻断内容传输。
阻断	识别出关键字后，阻断内容传输并记录日志。在用户看来则是无法显示网页、上传或下载文件失败、邮件发送或接收失败。
按权重操作	<p>每个关键字都存在一个权重值，当设备检测的内容中出现关键字时，设备会将这些关键字的权重值按出现次数累加。如果权重值的和大于等于“告警阈值”小于“阻断阈值”，则设备会执行“告警”动作，“告警”动作仅执行一次；如果权重值的和大于等于“阻断阈值”，则设备会执行“阻断”动作。</p> <p>例如：管理员在设备上定义了两个需要识别的关键字，关键字 a 的权重值为 1，关键字 b 的权重值为 2；定义了内容过滤的告警阈值为 1，阻断阈值为 5。如果设备检测出用户浏览的网页中存在一次关键字 a，这时权重值的和为 1，等于告警阈值 1，则设备会记录日志，用户仍然能正常浏览网页。如果设备检测出用户浏览的网页中出现了三次关键字 a 和两次关键字 b，这时权重值的和为 7 (<math>3 \times 1 + 2 \times 2 = 7</math>)，大于阻断阈值 5，则设备会阻断此网页并记录日志，用户看到的是无法显示网页。</p>

## 内容过滤处理流程

由[安全策略原理描述](#)可知，当通过设备的流量匹配了一条安全策略规则，规则的动作为 **permit** 且引用了内容过滤配置文件时，此流量需要进行内容过滤检测。

内容过滤的处理流程如下：

1. 设备对流量的内容进行检测，识别出流量的内容属性。

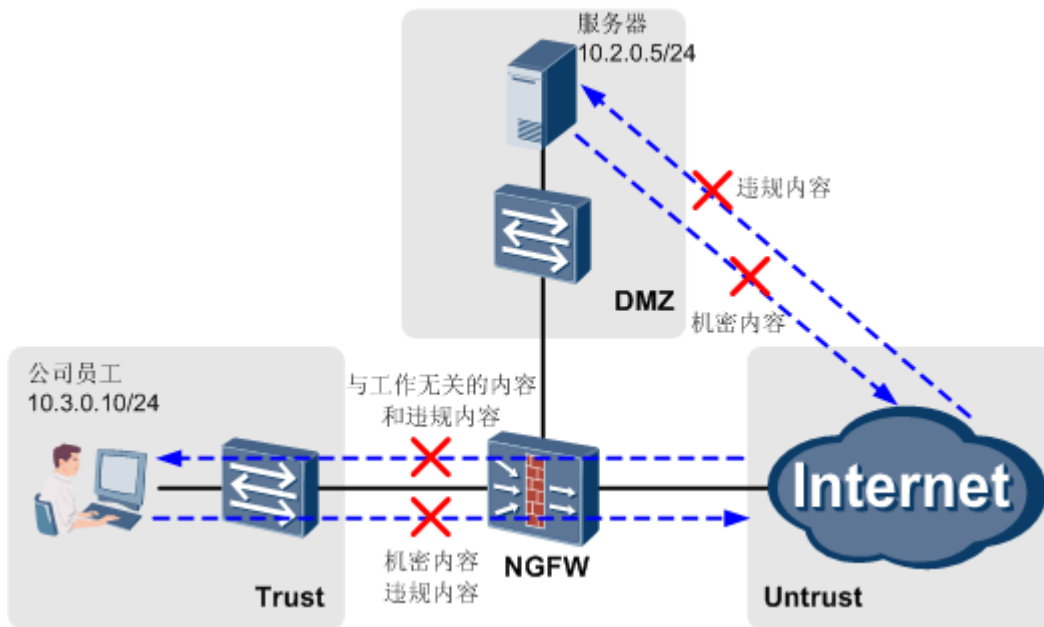
如果是应用内容则识别出应用的类型、应用内容传输的方向。如果是文件内容则识别出承载文件的应用类型，文件的类型和文件传输的方向。

2. 设备将流量的内容属性与内容过滤规则的条件进行匹配。如果所有条件都匹配，则此内容成功匹配此规则。如果其中有一个条件不匹配，则继续执行下一条规则。以此类推，如果所有内容过滤规则都不匹配，则设备允许此内容通过。
3. 如果内容成功匹配一条内容过滤规则，则设备会对此内容进行关键字检测，检测内容中是否存在内容过滤规则定义的关键字。如果检测时识别出关键字，则设备会执行响应动作。如果没有识别出关键字，则设备允许此内容通过。

## 内容过滤应用场景

内容过滤功能可以降低机密信息泄露的风险、防止违规信息的传播以及员工浏览和搜索与工作无关的内容。

图 1 内容过滤应用场景



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

- 降低公司机密泄露的风险。
  - 对内网用户上传的文件内容进行过滤，阻止内网用户上传包含公司机密信息的文件。
  - 对内网用户发送的邮件内容（包括标题、正文和附件）进行过滤，阻止内网用户发送包含公司机密信息的邮件。
  - 对内网用户发布的微博和帖子内容进行过滤，阻止内网用户发布包含公司机密信息的微博和帖子。
  - 对外网用户从内网服务器下载的文件内容进行过滤，防止黑客窃取包含公司机密信息的文件。
- 降低因员工浏览、发布、传播违规信息而给公司带来的法律风险。
  - 对内网用户上传和下载的文件内容进行过滤，阻止内网用户上传和下载包含违规信息的文件。
  - 对内网用户接收和发送的邮件内容（包括标题、正文和附件）进行过滤，阻止内网用户收发包含违规信息的邮件。
  - 对内网用户浏览网页的内容进行过滤，阻止内网用户浏览包含违规信息的网页。
  - 对内网用户搜索的内容进行过滤，阻止内网用户搜索违规信息。
  - 对内网用户发布的微博和帖子内容进行过滤，阻止内网用户发布包含违规信息的微博和帖子。
  - 对外网用户上传到内网服务器的文件内容进行过滤，防止外网用户将违规信息发送到公司服务器。

- 阻止员工浏览和搜索与工作无关的内容，提高工作效率。
  - 对内网用户浏览网页的内容进行过滤，阻止内网用户浏览与工作无关的网页。
  - 对内网用户搜索的内容进行过滤，阻止内网用户搜索与工作无关的内容。

## 使用限制和注意事项

配置内容过滤前请先阅读使用限制和注意事项。

配置内容过滤前，请注意以下事项：

- 对于文件中嵌套的文件不进行内容过滤。
- 对于 office 文件目前不支持对文件属性内容的过滤。
- 对于加密文件不进行内容过滤。
- 对于断点续传的文件不进行内容过滤。

## 配置关键字组

关键字组是内容过滤需要过滤的关键字的合集，在定义内容过滤配置文件前需要完成关键字组的配置。

### 背景信息

关键字组定义了内容过滤功能需要过滤的机密或违规的关键字。关键字组是由预定义关键字和自定义关键字组成的。

- 预定义关键字是指系统默认存在的可以检测的关键字，包括：银行卡号、信用卡号、社会安全号、身份证号、机密关键字（包括“秘密”、“机密”、“绝密”）。
- 自定义关键字是管理员自定义的需要检测的关键字，有文本和正则表达式两种方式。正则表达式的使用方法请参见[正则表达式规则](#)。

关键字组配置完成后需要在内容过滤配置文件的规则上引用。

NGFW 中存在一个缺省的关键字组，名称为 default，如下图所示。缺省关键字组不能被修改和删除。



名称	关键字				
	名称	描述	匹配模式	文本/正则表达式	权重
<input type="checkbox"/> default	银行卡号	匹配银行卡号	正则表达式	银行卡号	1
	信用卡号	匹配信用卡号	正则表达式	信用卡号	1
	社会安全号	匹配社会安全号	正则表达式	社会安全号	1
	身份证号	匹配身份证号	正则表达式	身份证号	1
	机密关键字	匹配机密关键字	正则表达式	机密关键字	1

## 操作步骤

1. 选择“对象 > 关键字组”。
2. 单击“新建”。
3. 配置关键字组的名称和描述。

参数	说明
名称	输入关键字组的名称。名称必须是唯一的，不能有重复的名称。当配置内容过滤时，名称会出现在“关键字组”的参数选择列表中。
描述	输入关键字组的描述信息。合理填写描述信息有助于管理员正确理解关键字组的功能，使关键字组变得方便选择、查找和维护。

4. 配置预定义关键字。

在“关键字列表”的“预定义”下可以看到设备支持的预定义关键字，包括：银行卡号、信用卡号、社会安全号、身份证号、机密关键字。

如果想要对预定义关键字进行过滤，则需要在其对应的“权重”输入框中输入权重值。如果“权重”输入框中显示为空，则不对此预定义关键字进行过滤。

5. 配置自定义关键字。
  - a. 在“关键字列表”中单击“新建”。
  - b. 配置自定义关键字的参数。

参数	说明
名称	输入自定义关键字的名称。名称必须是唯一的，不能有重复的名称。
描述	输入自定义关键字的描述信息。合理填写描述信息有助于管理员正确理解此自定义关键字的含义和作用。

参数	说明
匹配模式	选择自定义关键字的表示方式。 <ul style="list-style-type: none"> <li>文本：文本方式简单直观，适用于精确匹配的情况。</li> <li>正则表达式：一个正则表达式可以对应不同的内容，适用于模糊匹配的情况。</li> </ul>
文本	直接输入需要过滤的关键字，例如“abcde”、“#define”、“危险”等等。
正则表达式	使用正则表达式表示需要过滤的关键字。一个正则表达式可以表示多个关键字，因此更加灵活和高效，但是需要遵循 <a href="#">正则表达式规则</a> 。 例如“abc.de”可以匹配“abcade”、“abcyde”、“abc8de”等等。
权重	权重值代表了关键字的机密和重要程度。数值越大，关键字越重要。 当设备检测的内容中出现关键字时，设备会将这些关键字的权重值按出现次数累加。 <b>说明：</b> 如果“关键字组”中的多个“自定义关键字”能够表示相同的关键字，那么当设备检测到此关键字时，会将所有能够表示此关键字的“自定义关键字”的权重累加。 例如关键字“abc.de”和“abcde”都能表示“abcde”，那么当设备检测到出现一次“abcde”时，会将“abc.de”和“abcde”的权重相加。

c. 单击“确定”。

配置完成后，自定义关键字显示在“关键字列表”的“自定义”下。

d. 反复执行步骤 [5.a-5.c](#)，可以新建多个自定义关键字。

6. 单击“确定”，完成关键字组的配置。

7. 单击界面右上角的“提交”。

创建或修改关键字组后，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，建议您完成所有对关键字组的操作后再统一进行提交。

## 配置内容过滤

内容过滤配置文件决定了对哪些应用或文件类型进行过滤，定义内容过滤配置文件时需要引用关键字组。

### 前提条件

#### [配置关键字组](#)

## 背景信息

内容过滤包括文件内容过滤和应用内容过滤。

文件内容过滤是对用户上传和下载的文件内容中包含的关键字进行过滤。应用内容过滤是对应用协议中包含的关键字进行过滤。

NGFW 中存在一个内容过滤的缺省配置文件，名称为 default。缺省配置文件引用缺省关键字组，对 NGFW 支持的全部应用，全部文件类型的文件在上传方向上执行告警动作。缺省配置文件不能被修改和删除。

<input type="checkbox"/> 名称	规则名称	关键字组	应用	文件类型	方向	动作
<input type="checkbox"/> default	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，自定义关键字组，对每种应用或文件在上传/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 > 内容过滤”。
2. 单击“新建”。
3. 配置内容过滤配置文件的名称和描述。

参数	说明
名称	输入内容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“内容过滤”的参数选择列表中。
描述	输入内容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：阻断包含关键字组 1 的文档通过 FTP/SFTP 上传。

4. 配置内容过滤规则。
  - a. 在“内容过滤规则”中，单击“新建”。
  - b. 配置内容过滤规则的名称。

参数	说明
名称	输入内容过滤规则的名称。名称必须是唯一的，不能有重复的名称。

- c. 配置内容过滤规则的匹配条件，决定对哪些文件或应用进行检测。

设备将流量的内容属性与内容过滤规则的条件进行匹配。如果所有条件都匹配，则此内容成功匹配此规则。如果其中有一个条件不匹配，则继续执行下一条规则。以此类推，如果所有内容过滤规则都不匹配，则设备允许此内容通过。

参数	说明
应用	选择想要对哪些应用传输的文件内容进行过滤，或者对哪些应用本身的内容进行过滤。 <ul style="list-style-type: none"> <li>如果想要对文件内容进行过滤，则需要在“文件类型”中选择需要过滤的文件类型。</li> <li>如果想要对应用内容进行过滤，则需要在“文件类型”中选择“TEXT/HTML”。</li> </ul>
文件类型	选择想要对哪些类型的文件内容进行过滤。如果需要对协议内容进行过滤，请选择“TEXT/HTML”。
方向	选择想要对哪个方向传输的文件内容或协议内容进行过滤。 上传是指用户将内容从源地址发送到目的地址，下载是指用户将内容从目的地址接收到源地址。

d. 配置内容过滤规则的关键字组，决定要检测出哪些关键字。

如果内容成功匹配一条内容过滤规则，则设备会对此内容进行关键字检测，检测内容中是否存在内容过滤规则定义的关键字。如果检测时识别出关键字，则设备会执行响应动作。如果没有识别出关键字，则设备允许此内容通过。

参数	说明
关键字组	通过选择关键字决定需要对哪些内容即关键字进行过滤。关键字组是关键字的合集，包括预定义和自定义关键字。预定义包括银行卡号、信用卡号、社会安全号、身份证号、机密关键词。自定义关键字是由管理员自行定义的需要过滤的关键字。关键字组的配置请参见 <a href="#">配置关键字组</a> 。

e. 配置内容过滤规则的响应动作。



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”或权重值大于等于“阻断阈值”时，设备将执行告警动作。

参数	说明
动作	当内容匹配全部条件且检测出关键字时设备执行的动作。 <ul style="list-style-type: none"> <li>告警：允许内容传输并记录日志。</li> <li>阻断：默认动作，阻断内容传输并记录日志。</li> </ul>

参数	说明
	<ul style="list-style-type: none"> <li>按权重操作：关键字组中每个关键字都存在一个权重值，当设备检测的内容中出现关键字时，设备会将这些关键字的权重值按出现次数累加。 <ul style="list-style-type: none"> <li>如果权重值的和小于“告警阈值”，则设备会允许此内容的传输。</li> <li>如果权重值的和大于等于“告警阈值”且小于“阻断阈值”，则设备会执行动作“告警”，“告警”动作仅执行一次。</li> <li>如果权重值的和大于等于“阻断阈值”，则设备会执行动作“阻断”。</li> </ul> </li> </ul>

f. 单击“确定”。

g. 反复执行步骤 a-f，可以新建多个内容过滤规则。

5. 单击“确定”，完成内容过滤配置文件的配置。

6. 在安全策略中引用内容过滤配置文件。关于安全策略的具体配置请参见[配置安全策略](#)。

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：配置内容过滤

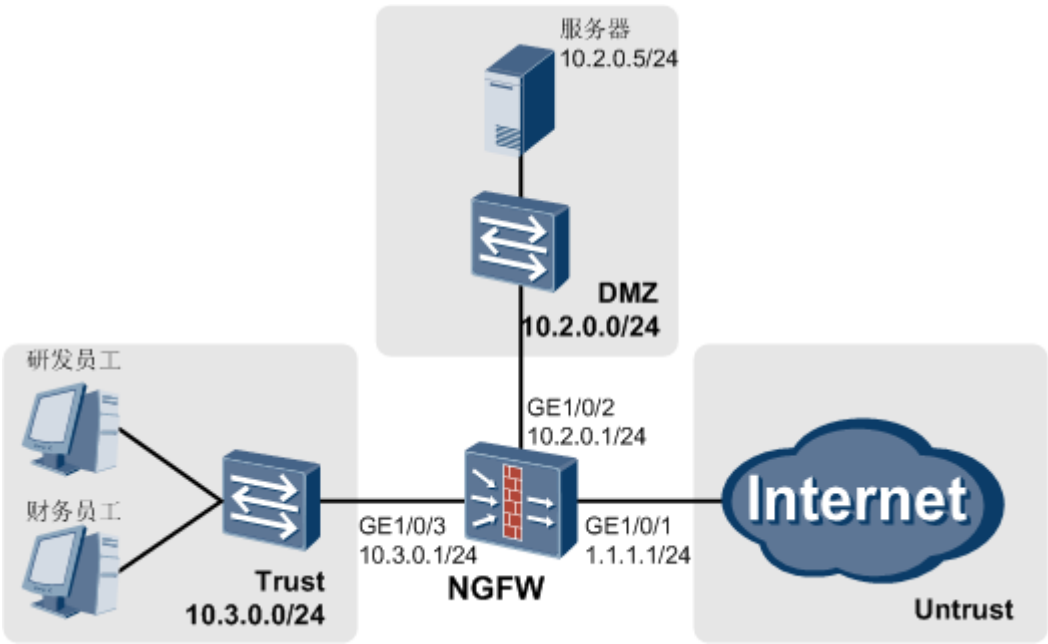
在企业网关配置内容过滤后，既可以防止公司内的机密信息被泄露到外部，又可以防止违规信息的传播。

## 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。公司有研发和财务两种用户，都部署在 Trust 区域。公司的内网服务器部署在 DMZ 区域。Internet 的用户部署在 Untrust 区域。

公司希望在保证网络正常使用的同时，防止公司机密信息的泄露以及违规信息的传播。

图 1 内容过滤组网图



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
研发员工的安全策略	<ul style="list-style-type: none"><li>名称：policy_sec_research</li><li>源安全区域：trust</li><li>目的安全区域：untrust</li><li>用户：research</li><li>动作：允许</li><li>内容过滤：profile_data_research</li></ul>	安全策略“policy_sec_research”的作用是允许研发员工访问 Internet，引用内容过滤配置文件“profile_sec_research”可以对研发员工上传到 Internet 的文件、发送到 Internet 的邮件、发布的帖子和微博、浏览网页和搜索的内容进行过滤。
财务员工的安全策略	<ul style="list-style-type: none"><li>名称：policy_sec_finance</li><li>源安全区域：trust</li><li>目的安全区域：untrust</li><li>用户：finance</li><li>动作：允许</li><li>内容过滤：profile_data_finance</li></ul>	安全策略“policy_sec_finance”的作用是允许财务员工访问 Internet，引用内容过滤配置文件“profile_sec_finance”可以对财务员工上传到 Internet 的文件、发送到 Internet 的邮件、发布的帖子和微博、浏览网页和搜索的内容进行过滤。
Internet 用户的安全策略	<ul style="list-style-type: none"><li>名称：policy_sec_internet</li><li>源安全区域：untrust</li><li>目的安全区域：dmz</li></ul>	安全策略“policy_sec_internet”的作用是允许 Internet 用户访问内网服务器，引用内容过滤配置文件“profile_sec_internet”可以对 Internet 用户从内

项目	数据	说明
	<ul style="list-style-type: none"> <li>目的地址/地区: 10.2.0.5/24</li> <li>动作: 允许</li> <li>内容过滤: profile_data_internet</li> </ul>	网服务器下载和上传到内网服务器的文件内容进行过滤。
研发员工的内容过滤配置文件	名称: profile_data_research	内容过滤配置文件“profile_data_research”需要应用在安全策略“policy_sec_research”上。
	<ul style="list-style-type: none"> <li>名称: rule1</li> <li>关键字组: keyword1</li> <li>应用: all</li> <li>文件类型: all</li> <li>方向: 上传</li> <li>动作: 阻断</li> </ul>	规则“rule1”的作用是阻断包含关键字组“keyword1”的内容的上传。
	<ul style="list-style-type: none"> <li>名称: rule2</li> <li>关键字组: keyword3</li> <li>应用: HTTP</li> <li>文件类型: TEXT/HTML</li> <li>方向: 下载</li> <li>动作: 阻断</li> </ul>	规则“rule2”的作用是阻断包含关键字组“keyword3”内容的网页和搜索。
财务员工的内容过滤配置文件	名称: profile_data_finance	内容过滤配置文件“profile_data_finance”需要应用在安全策略“policy_sec_finance”上。
	<ul style="list-style-type: none"> <li>名称: rule1</li> <li>关键字组: keyword2</li> <li>应用: all</li> <li>文件类型: all</li> <li>方向: 上传</li> <li>动作: 阻断</li> </ul>	规则“rule1”的作用是阻断包含关键字组“keyword2”的内容的上传。
	<ul style="list-style-type: none"> <li>名称: rule2</li> <li>关键字组: keyword3</li> <li>应用: HTTP</li> <li>文件类型: TEXT/HTML</li> <li>方向: 下载</li> <li>动作: 阻断</li> </ul>	规则“rule2”的作用是阻断包含关键字组“keyword3”内容的网页和搜索。
Internet 用户的内容过滤配置文件	名称: profile_data_internet	内容过滤配置文件“profile_data_internet”需要应用在安全策略“policy_sec_internet”上。
	<ul style="list-style-type: none"> <li>名称: rule1</li> <li>关键字组: keyword2</li> <li>应用: all</li> <li>文件类型: all</li> <li>方向: 下载</li> <li>动作: 阻断</li> </ul>	规则“rule1”的阻断包含关键字组“keyword2”内容的文件下载。
	<ul style="list-style-type: none"> <li>名称: rule2</li> </ul>	规则“rule2”的阻断包含关键字组“keyword3”内

项目	数据	说明
	<ul style="list-style-type: none"> <li>关键字组: keyword3</li> <li>应用: all</li> <li>文件类型: all</li> <li>方向: 上传</li> <li>动作: 阻断</li> </ul>	容的文件上传。
keyword1	预定义关键字: 机密关键字 (权重设置为 1)	-
	自定义关键字: <ul style="list-style-type: none"> <li>公司机密信息               <ul style="list-style-type: none"> <li>名称: 公司机密信息</li> <li>匹配模式: 文本</li> <li>文本: “公司机密”</li> <li>权重: 1</li> </ul> </li> <li>公司违规信息               <ul style="list-style-type: none"> <li>名称: 公司违规信息</li> <li>匹配模式: 文本</li> <li>文本: “违规信息”</li> <li>权重: 1</li> </ul> </li> </ul>	“公司机密”是由公司定义的机密信息关键字, 请管理员根据实际情况确定具体内容。本举例中仅以“公司机密”表示。 “违规信息”是由公司定义的违规信息关键字, 可能包括敏感、色情、暴力等信息, 请管理员根据实际情况确定具体内容。本举例中仅以“违规信息”表示。
keyword2	预定义关键字 (权重都设置为 1): 银行卡号、信用卡号、社会安全号、身份证号、机密关键字。	-
	自定义关键字: <ul style="list-style-type: none"> <li>公司机密信息               <ul style="list-style-type: none"> <li>名称: 公司机密信息</li> <li>匹配模式: 文本</li> <li>文本: “公司机密”</li> <li>权重: 1</li> </ul> </li> <li>公司违规信息               <ul style="list-style-type: none"> <li>名称: 公司违规信息</li> <li>匹配模式: 文本</li> <li>文本: “违规信息”</li> <li>权重: 1</li> </ul> </li> </ul>	“公司机密”是由公司定义的机密信息关键字, 请管理员根据实际情况确定具体内容。本举例中仅以“公司机密”表示。 “违规信息”是由公司定义的违规信息关键字, 可能包括敏感、色情、暴力等信息, 请管理员根据实际情况确定具体内容。本举例中仅以“违规信息”表示。
keyword3	自定义关键字: 公司违规信息 <ul style="list-style-type: none"> <li>名称: 公司违规信息</li> <li>匹配模式: 文本</li> <li>文本: “违规信息”</li> <li>权重: 1</li> </ul>	-

## 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. 新建关键字组 keyword1、keyword2、keyword3，便于下面步骤中的内容过滤配置文件引用。
3. 为研发员工、财务员工、Internet 用户分别新建内容过滤配置文件。新建内容过滤配置文件时需要引用关键字组。
4. 为研发员工、财务员工、Internet 用户分别配置安全策略，在保证网络可达的同时引用各自的内容过滤配置文件，实现内容过滤。

## 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. 新建关键字组。

- a. 选择“对象 > 关键字组”。
- b. 在“关键字组”中单击“新建”。
- c. 在“名称”中输入“keyword1”。
- d. 在“预定义”下的“机密关键字”对应的“权重”输入框中分别输入“1”。
- e. 在“关键字列表”中单击“新建”。
- f. 按照如下参数配置自定义关键字“公司机密信息”。

名称	公司机密信息
匹配模式	文本
文本	“公司机密”
权重	1

- g. 单击“确定”，完成自定义关键字“公司机密信息”的配置。
- h. 在“关键字列表”中单击“新建”。
- i. 按照如下参数配置自定义关键字“公司违规信息”。

名称	公司违规信息
匹配模式	文本
文本	“违规信息”
权重	1

- j. 单击“确定”，完成自定义关键字“公司违规信息”的配置。
- k. 单击“确定”，完成关键字组 keyword1 的配置。
- l. 参考上述步骤按照下图所示参数配置 keyword2。

名称
keyword2
\*

描述

关键字列表

+ 新建
X 删除

<input type="checkbox"/> 名称	描述	匹配模式	文本/正则表达式	权重<0-255> ?
自定义				
<input type="checkbox"/> 公司违规信息		文本	“违规信息”	1
<input type="checkbox"/> 公司机密信息		文本	“公司机密”	1
预定义				
<input type="checkbox"/> 银行卡号	匹配银行卡号	正则表达式	银行卡号	1
<input type="checkbox"/> 信用卡号	匹配信用卡号	正则表达式	信用卡号	1
<input type="checkbox"/> 社会安全号	匹配社会安全号	正则表达式	社会安全号	1
<input type="checkbox"/> 身份证号	匹配身份证号	正则表达式	身份证号	1
<input type="checkbox"/> 机密关键字	匹配机密关键字	正则表达式	机密关键字	1

- m. 参考上述步骤按照下图所示参数配置 keyword3。

名称 keyword3 \*

描述

**关键字列表**

+ 新建 ✕ 删除

<input type="checkbox"/> 名称	描述	匹配模式	文本/正则表达式	权重<0-255> (?)
自定义				
<input type="checkbox"/> 公司违规信息		文本	“违规信息”	1
预定义				

3. 新建内容过滤配置文件。

- 选择“对象 > 安全配置文件 > 内容过滤”。
- 单击“新建”。
- 输入“名称”为“profile\_data\_research”。
- 单击“新建”。
- 按照如下参数配置研发员工的内容过滤配置文件 profile\_data\_research 的规则 rule1。

名称	rule1
关键字组	keyword1
应用	all
文件类型	all
方向	上传
动作	阻断

- 单击“确定”。
- 参考上述步骤按如下参数配置规则 rule2。

名称	rule2
关键字组	keyword3
应用	HTTP
文件类型	TEXT/HTML
方向	下载
动作	阻断

- 单击“确定”，完成“profile\_data\_research”的配置。
- 参考上述步骤按如下参数配置财务员工的内容过滤配置文件 profile\_data\_finance。

名称	profile_data_finance
内容过滤规则	
rule1	<ul style="list-style-type: none"> <li>名称: rule1</li> <li>关键字组: keyword2</li> <li>应用: all</li> <li>文件类型: all</li> <li>方向: 上传</li> <li>动作: 阻断</li> </ul>
rule2	<ul style="list-style-type: none"> <li>名称: rule2</li> <li>关键字组: keyword3</li> <li>应用: HTTP</li> <li>文件类型: TEXT/HTML</li> <li>方向: 下载</li> <li>动作: 阻断</li> </ul>

j. 参考上述步骤按如下参数配置 Internet 用户的内容过滤配置文件 profile\_data\_internet。

名称	profile_data_internet
内容过滤规则	
rule1	<ul style="list-style-type: none"> <li>名称: rule1</li> <li>关键字组: keyword2</li> <li>应用: all</li> <li>文件类型: all</li> <li>方向: 下载</li> <li>动作: 阻断</li> </ul>
rule2	<ul style="list-style-type: none"> <li>名称: rule2</li> <li>关键字组: keyword3</li> <li>应用: all</li> <li>文件类型: all</li> <li>方向: 上传</li> <li>动作: 阻断</li> </ul>

4. 配置安全策略并引用内容过滤配置文件。

- 选择“策略 > 安全策略 > 安全策略”。
- 单击“新建”。
- 按照如下参数配置研发员工的安全策略。

名称	policy_sec_research
描述	允许研发员工访问 Internet
源安全区域	trust

目的安全区域	untrust
用户	/default/research
动作	允许
内容过滤	profile_data_research

d. 单击“确定”。

e. 参考上述步骤按如下参数配置财务员工的安全策略。

名称	policy_sec_finance
描述	允许财务员工访问 Internet
源安全区域	trust
目的安全区域	untrust
用户	/default/finance
动作	允许
内容过滤	profile_data_finance

f. 参考上述步骤按如下参数配置 Internet 用户的安全策略。

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
内容过滤	profile_data_internet

5. 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

1. 内网研发员工发送包含公司机密信息的内容到 Internet 或者浏览和搜索包含违规信息的内容时，内容被阻断。
2. 内网财务员工发送包含公司机密信息和员工信息的内容到 Internet 或者浏览和搜索包含违规信息的内容时，内容被阻断。
3. Internet 用户从内网服务下载包含公司机密信息和员工信息的文件时，下载文件失败。Internet 用户上传包含违规信息的文件到内网服务器时，上传文件失败。

4. 如果想查看内容阻断时的日志详细信息，可以查看“内容日志”。方法如下：

- a. 选择“监控 > 日志 > 内容日志”。
- b. 单击“高级查询”，选择“类型”为“内容过滤”。
- c. 单击“查询”，可以看到内容过滤功能的日志。

## 配置脚本

```
keyword-group name keyword1
pre-defined-keyword name confidentiality weight 1
user-defined-keyword name 公司机密信息
expression match-mode text “公司机密”
weight 1
user-defined-keyword name 公司违规信息
expression match-mode text “违规信息”
weight 1
keyword-group name keyword2
pre-defined-keyword name bank-card-number weight 1
pre-defined-keyword name credit-card-number weight 1
pre-defined-keyword name social-security-number weight 1
pre-defined-keyword name id-card-number weight 1
pre-defined-keyword name confidentiality weight 1
user-defined-keyword name 公司机密信息
expression match-mode text “公司机密”
weight 1
user-defined-keyword name 公司违规信息
expression match-mode text “违规信息”
weight 1
keyword-group name keyword3
user-defined-keyword name 公司违规信息
expression match-mode text “违规信息”
weight 1
profile type data-filter name profile_data_research
rule name rule1
keyword-group name keyword1
file-type all
application all
direction upload
action block
rule name rule2
keyword-group name keyword3
```

```

file-type name TEXT/HTML
application type HTTP
direction download
action block
profile type data-filter name profile_data_finance
rule name rule1
keyword-group name keyword2
file-type all
application all
direction upload
action block
rule name rule2
keyword-group name keyword3
file-type name TEXT/HTML
application type HTTP
direction download
action block
profile type data-filter name profile_data_internet
rule name rule1
keyword-group name keyword2
file-type all
application all
direction download
action block
rule name rule2
keyword-group name keyword3
file-type all
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_research
  source-zone trust
  destination-zone untrust
  user /default/research
  profile data-filter profile_data_research
  action permit
rule name policy_sec_finance
  source-zone trust
  destination-zone untrust
  user /default/finance
  profile data-filter profile_data_finance
  action permit
rule name policy_sec_internet
  source-zone untrust
  destination-zone dmz
  destination-address 10.2.0.0 24
  profile data-filter profile_data_internet
  action permit
```

## 配置的内容过滤没有生效

配置内容过滤后，某些应该被过滤掉的内容仍然能正常显示或出现在文件中。

### 现象描述

NGFW 上配置了内容过滤功能，想要阻断包含特定关键字的内容在安全区域间的传输。但是当管理员进行测试的时候发现，应该被阻断的内容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内容过滤配置文件。



原因三：内容过滤规则的匹配条件配置错误。

原因四：关键字组配置错误，没有定义想要过滤的关键字。

原因五：内容过滤规则的“动作”为“告警”。

原因六：内容过滤规则的“动作”为“按权重操作”，但关键字的权重和小于“阻断阈值”。

## 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内容过滤配置文件。

- 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“内容过滤”配置文件。
  - 如果安全策略没有引用或者引用的不是正确的“内容过滤”配置文件，则选择在配置规划时此安全策略计划引用的“内容过滤”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：内容过滤配置文件的匹配条件配置错误。

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

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

- 如果内容过滤规则的条件配置不正确，则修改内容过滤规则。
- 如果内容过滤规则的条件配置正确，则执行 4。

4. 原因四：关键字组配置错误，没有定义想要过滤的关键字。

- a. 选择“对象 > 关键字组”。
- b. 单击内容过滤配置文件引用的关键字组，查看“关键字列表”中的自定义和预定义关键字是否包含需要过滤的内容。
  - 如果不包含，则修改关键字组的配置，使其包含需要过滤的内容。
  - 如果包含，则执行 5 或 6。

5. 原因五：内容过滤规则的“动作”为“告警”。

- a. 在“修改内容过滤配置文件”界面查看各内容过滤规则的动作。
  - 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但记录日志是正常的情况。
  - 如果“动作”为“告警”，但配置规划时计划的“动作”为“阻断”或“按权重操作”，则需要修改内容过滤规则的动作。

6. 原因六：内容过滤规则的“动作”为“按权重操作”，但关键字的权重和小于“阻断阈值”。

#### 说明：

管理员修改阻断阈值和关键字权重值时，需要反复测试和调整。

- a. 选择“对象 > 安全配置文件 > 内容过滤”，查看“阻断阈值”的大小。如果数值过大则调小“阻断阈值”。
- b. 选择“对象 > 关键字组”，查看关键字的权重。如果数值过小则调大权重值。

## 配置了内容过滤后影响了正常内容的传输

配置了内容过滤后，正常的上传和下载操作不能进行。

## 现象描述

NGFW 上配置了内容过滤功能，想要阻断包含特定关键字的内容在安全区域间的传输。但是内网用户在使用时发现不包含关键字的内容也无法正常传输。

## 可能原因

原因一：流量没有匹配正确的安全策略。

原因二：流量被其他内容安全功能阻断。

原因三：内容过滤配置文件配置错误。

原因四：关键字组配置错误。

原因五：关键字权重取值过大或“阻断阈值”取值过小。

## 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。
- 如果流量被内容过滤配置文件阻断，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：内容过滤配置文件配置错误。
- a. 单击 [2](#) 中查询到的内容过滤配置文件的名称，在“修改内容过滤配置文件”界面查看内容过滤规则。
- b. 调整内容过滤规则的参数，保证内容过滤规则的条件不匹配正常的内容传输条件。
4. 原因四：关键字组配置错误。
- a. 选择“对象 > 关键字组”。
- b. 单击内容过滤配置文件引用的关键字组，查看“关键字列表”中的自定义和预定义关键字是否包含了不需要过滤的内容。
- 如果包含，则修改关键字组的配置，使其不包正常的内容。
  - 如果不包含，则执行 [5](#)。
5. 原因五：关键字权重取值过大或“阻断阈值”取值过小。



#### 说明：

管理员修改阻断阈值和关键字权重值时，需要反复测试和调整。

- a. 选择“对象 > 安全配置文件 > 内容过滤”，查看“阻断阈值”的大小。如果数值过小则调大“阻断阈值”。
- b. 选择“对象 > 关键字组”，查看关键字的权重。如果数值过大则调小权重值。

## 内容过滤 FAQ

内容过滤特性常见疑问的回答。

身份证号或银行卡的数字间如果加入空格或分隔符是否还能够进行过滤？

不能进行过滤。

访问的网页或搜索内容中如果包含过滤的内容，网页将如何显示？

显示“无法打开网页”。

如果发布的帖子或微博中包含过滤的内容，网页将如何显示？

显示“无法打开网页”。

## HCIE-Security 模拟面试问题及面试建议

1. 内容过滤处理流程是什么？