

# HCIE-Security 备考指南

## 应用行为控制



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 应用行为控制需要掌握的知识点.....	1
应用行为控制简介 .....	1
应用行为控制应用场景.....	2
使用限制和注意事项 .....	3
配置应用行为控制.....	3
举例：配置应用行为控制.....	5
HCIE-Security 模拟面试问题及面试建议 .....	12

## HCIE-Security 应用行为控制需要掌握的知识点

- 熟悉应用行为控制关键技术
- 掌握应用行为控制技术的应用

### 应用行为控制简介

NGFW 的应用行为控制功能用来对用户的 HTTP 行为和 FTP 行为进行精确的控制。

与传统设备使用协议或端口号来控制 HTTP 和 FTP 协议不同，NGFW 的应用行为控制功能可以对 HTTP 和 FTP 进行更精细的控制。例如，您可以通过应用行为控制功能禁止 FTP 的文件上传和文件删除操作，但允许 FTP 文件下载操作。应用行为控制包含的控制项说明如表 1 所示。

表 1 应用行为控制项说明			
行为类型	控制项	说明	动作
HTTP 行为	POST 操作	HTTP POST 一般用于通过网页向服务器发送信息，例如论坛发帖、表单提交、用户名/密码登录。	允许/禁止
	浏览网页	采用浏览器进行网页浏览。	
	代理上网	代理上网是指用户使用代理服务器访问特定网站，使用该功能时 NGFW 需部署在内网用户和代理服务器之间。	
	文件上传	-	
	文件下载	-	
	文件上传大小（告警/阻断阈值）	当允许文件上传操作时，可以配置告警阈值 <sup>a</sup> 和阻断阈值 <sup>b</sup> ，对上传的文件大小进行控制。	告警/阻断
	文件下载大小（告警/阻断阈值）	当允许文件下载操作时，可以配置告警阈值 <sup>a</sup> 和阻断阈值 <sup>b</sup> ，对下载的文件大小进行控制。 HTTP 文件下载控制项用来	

表 1 应用行为控制项说明			
行为类型	控制项	说明	动作
		控制采用 HTTP 协议进行文件下载的操作，如在文件下载页面选择专用的下载工具（如 BT、电驴等）进行下载，将无法对下载工具进行控制。	
FTP 行为	文件上传	-	允许/禁止
	文件下载	-	
	文件删除	-	
	文件上传大小（告警/阻断阈值）	当允许文件上传操作时，可以配置告警阈值 <sup>a</sup> 和阻断阈值 <sup>b</sup> ，对上传的文件大小进行控制。	告警/阻断
	文件下载大小（告警/阻断阈值）	当允许文件下载操作时，可以配置告警阈值 <sup>a</sup> 和阻断阈值 <sup>b</sup> ，对下载的文件大小进行控制。	

a：当上传或下载的文件大小达到告警阈值时，系统会产生日志信息对设备管理员进行提示。

b：当上传或下载的文件大小达到阻断阈值时，系统将阻断上传或下载的文件，并产生日志信息对设备管理员进行提示。

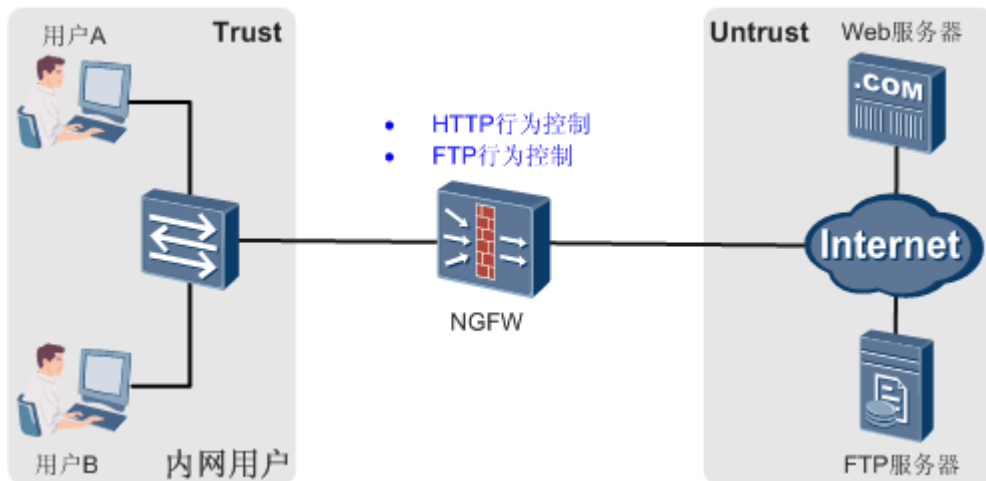
在创建安全策略时，可以把应用行为控制配置文件同用户、时间段等对象结合起来，达到不同用户、不同时间段的应用行为差异化管理的目的。

## 应用行为控制应用场景

应用行为控制常用于企业内部对内网用户的上网（HTTP）行为和 FTP 行为进行管理。

在企业内部通常需要对内网用户的 HTTP 行为和 FTP 行为进行管理，不同的用户使用 HTTP 和 FTP 访问网络资源需要不同的权限，同一用户在不同的时间段具有的权限往往也不同。NGFW 的应用行为控制能够很好的满足上述需求，其典型组网如[图 1](#)所示。

图 1 应用行为控制典型应用场景



NGFW 作为企业的出口网关部署在内网出口处，通过在 NGFW 上配置应用行为控制功能，当内网用户访问外网时，能够有效管理内网用户的 HTTP 行为和 FTP 行为。

在 NGFW 上创建多个应用行为控制配置文件，每个应用行为控制配置文件用来控制用户具有不同的 HTTP 和 FTP 权限。然后通过安全策略里面引用应用行为控制配置文件、用户和时间段（工作时间、非工作时间）等对象，可以达到对内网用户的 HTTP 行为和 FTP 行为差异化、精细化管理的目的。

## 使用限制和注意事项

配置应用前请先阅读使用限制和注意事项。

### 使用限制

- 文件上传大小/文件下载大小限制对支持断点续传的文件上传/下载无效。
- HTTP 文件下载控制项用来控制采用 HTTP 协议进行文件下载的操作，如在文件下载页面选择专用的下载工具（如 BT、电驴等）进行下载，将无法对下载工具进行控制。









## 配置应用行为控制

介绍了应用行为控制的配置步骤。

### 背景信息

为了达到应用行为差异化管理的目的，往往需要配置多个应用行为控制配置文件，请您根据应用行为控制的需要合理规划每个配置文件里的允许和禁止项。

NGFW 中存在一个应用行为控制的缺省配置文件，名称为 default。缺省配置文件中已经定义了每种协议在上传或下载方向上的缺省动作，如下所示。缺省配置文件不能被修改和删除。

名称	HTTP					FTP		
	POST操作	浏览网页	代理上网	文件上传	文件下载	文件上传	文件下载	文件删除
default								

NGFW 支持创建自定义配置文件，您可以根据需要，对每种协议应用不同的响应动作。

## 操作步骤

1. 选择“对象 > 安全配置文件 > 应用行为控制”。
2. 单击“新建”。
3. 配置应用行为控制配置文件。

参数	说明
名称	输入应用行为控制的名称。
描述	输入应用行为控制的描述信息。为了方便识别该应用行为控制配置文件的用途，建议输入的描述信息应具有一定的意义。
<b>HTTP 行为控制</b>	
HTTP POST 操作	HTTP POST 一般用于通过网页向服务器发送信息，例如论坛发帖、表单提交、用户名/密码登录。
HTTP 浏览网页	采用浏览器进行网页浏览。
HTTP 代理上网	代理上网是指用户使用代理服务器访问特定网站，使用该功能时 NGFW 需部署在内网用户和代理服务器之间。
HTTP 文件上传	当允许文件上传操作时，可以配置告警阈值 <sup>a</sup> 和阻断阈值 <sup>b</sup> ，对上传的文件大小进行控制。
HTTP 文件下载	当允许文件下载操作时，可以配置告警阈值 <sup>a</sup> 和阻断阈值 <sup>b</sup> ，对下载的文件大小进行控制。 该控制项用来控制采用 HTTP 协议进行文件下载的操作，如在文件下载页面选择专用的下载工具（如 BT、电驴等）进行下载，将无法对下载工具进行控制。
<b>FTP 行为控制</b>	
FTP 文件上传	当允许文件上传操作时，可以配置告警阈值 <sup>a</sup> 和阻断阈值 <sup>b</sup> ，对上传的文件大小进行控制。
FTP 文件下载	当允许文件下载操作时，可以配置告警阈值 <sup>a</sup> 和阻断阈值 <sup>b</sup> ，对下载的文件大小进行控制。

参数	说明
FTP 文件删除	-

a: 当上传或下载的文件大小达到告警阈值时，系统会产生日志信息对设备管理员进行提示。

b: 当上传或下载的文件大小达到阻断阈值时，系统将阻断上传或下载的文件，并产生日志信息对设备管理员进行提示。

#### 说明:

缺省情况下，系统未配置告警阈值和阻断阈值，不对上传或下载的文件大小进行控制。

可以单独配置告警阈值或阻断阈值，也可以同时配置告警阈值和阻断阈值。同时配置告警阈值和阻断阈值时，告警阈值必须小于阻断阈值。

4. 单击“确定”。
5. 在安全策略中引用应用行为控制配置文件。

### 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：配置应用行为控制

在企业安全网关上配置应用行为控制功能，可以管理内网用户的上网（HTTP）行为和 FTP 行为。

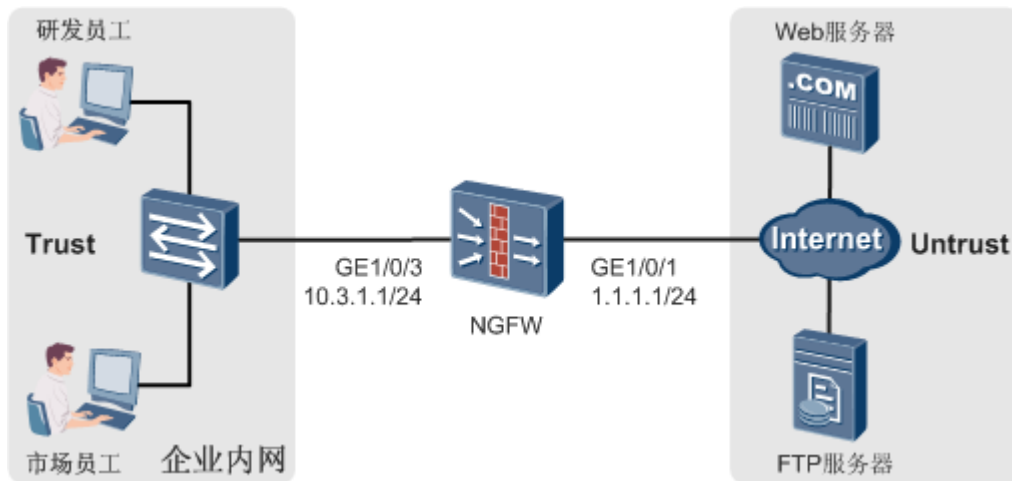
### 组网需求

如图 1 所示，NGFW 做为企业的出口网关部署在内网出口处，企业内网员工按工作职能分为研发员工和市场员工。其中，研发员工所属的研发用户组（research）和市场员工所属的市场用户组（marketing）已经创建，并已经完成认证的相关配置。现要求在 NGFW 上配置应用行为控制功能，对研发员工和市场员工访问外网的 HTTP 行为和 FTP 行为进行控制：

- 研发员工在工作时间（工作日的 09:00:00~17:00:00）禁止任何 HTTP 和 FTP 操作，避免影响工作效率。

- 研发员工在非工作时间（双休日、工作日的非工作时间）允许 HTTP 浏览网页、HTTP 代理上网和 HTTP 文件下载，其余 HTTP 权限和 FTP 权限全部禁止。
- 市场员工有对外交流的需求，同时出于信息安全的考虑，只对 HTTP 和 FTP 上传的文件大小进行控制，禁止 HTTP 和 FTP 上传超过 100M 的文件，其余功能不受控制。

图 1 应用行为控制组网图



## 数据规划

项目	数据	说明
应用行为控制配置文件	<ul style="list-style-type: none"> <li>名称： profile_app_research_work</li> <li>控制项：HTTP 行为和 FTP 行为的所有控制项全部禁止</li> </ul>	用来控制研发员工在工作时间段的 HTTP 行为和 FTP 行为。
	<ul style="list-style-type: none"> <li>名称： profile_app_research_rest</li> <li>控制项：只允许 HTTP 浏览网页、HTTP 代理上网、HTTP 文件下载</li> </ul>	用来控制研发员工在非工作时间的 HTTP 和 FTP 行为。
	<ul style="list-style-type: none"> <li>名称： profile_app_marketing</li> <li>控制项：HTTP 行为和 FTP 行为的所有控制项全部允许，HTTP 文件上传和 FTP 文件上传的阻断阈值为 102400KB（100M）</li> </ul>	用来控制市场员工的 FTP 行为。
安全策略	<ul style="list-style-type: none"> <li>名称： policy_sec_research_work</li> <li>源安全区域：trust</li> </ul>	允许研发员工访问外网，通过引用时间段“working_hours”和应用行为控制配置文件“profile_app_research_work”用来控制研



项目	数据	说明
	<ul style="list-style-type: none"> <li>目的安全区域: untrust</li> <li>员工: research (研发用户组)</li> <li>时间段: working_hours (09:00:00 - 17:00:00/工作日)</li> <li>动作: permit</li> <li>应用行为控制: profile_app_research_work</li> </ul>	发员工在工作时间段的应用行为。
	<ul style="list-style-type: none"> <li>名称: policy_sec_research_rest</li> <li>源安全区域: trust</li> <li>目的安全区域: untrust</li> <li>员工: research (研发用户组)</li> <li>时间段: off_hours (双休日、工作日的 00:00:00 - 08:59:59、工作日的 17:01:00 - 23:59:59)</li> <li>动作: permit</li> <li>应用行为控制: profile_app_research_rest</li> </ul>	允许研发员工访问外网, 通过引用时间段“off_hours”以及应用行为控制配置文件“profile_app_research_rest”用来控制研发员工在非工作时间段的应用行为。
	<ul style="list-style-type: none"> <li>名称: policy_sec_marketing</li> <li>源安全区域: trust</li> <li>目的安全区域: untrust</li> <li>员工: marketing (市场用户组)</li> <li>动作: permit</li> <li>应用行为控制: profile_app_marketing</li> </ul>	允许市场员工访问外网, 通过引用应用行为控制配置文件“profile_app_marketing”, 用来控制市场员工的应用行为。

## 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, 按如下参数配置。

安全区域	untrust
IPv4	
IP 地址	1.1.1.1/24

- c. 单击“确定”。
- d. 参考上述步骤按如下参数配置 GE1/0/3 接口。

安全区域	trust
IPv4	
IP 地址	10.3.1.1/24

2. 新建三个应用行为控制配置文件，研发员工在工作时间段使用的配置文件名称为“profile\_app\_research\_work”，研发员工在非工作时间段使用的配置文件名称为“profile\_app\_research\_rest”，市场员工使用的配置文件名称为“profile\_app\_marketing”。
  - a. 选择“对象 > 安全配置文件 > 应用行为控制”。
  - b. 单击“新建”，创建名称为“profile\_app\_research\_work”的配置文件，配置文件里面的控制项全部修改为“禁止”。
  - c. 单击“确定”。
  - d. 参考上述步骤，创建名称为“profile\_app\_research\_rest”的配置文件，只允许 HTTP 浏览网页、HTTP 代理上网和 HTTP 文件下载，其余控制项全部修改为禁止。
  - e. 参考上述步骤，创建名称为“profile\_app\_marketing”的配置文件，HTTP 行为和 FTP 行为的所有控制项全部允许，按如下参数配置 HTTP 文件上传和 FTP 文件上传的阻断阈值。

HTTP 文件上载	阻断阈值：102400KB
FTP 文件上载	阻断阈值：102400KB

3. 创建名称为 working\_hours 的时间段，该时间段为工作时间，对应工作日的 09:00:00 – 17:00:00。
  - a. 选择“对象 > 时间段”。
  - b. 单击“新建”，按如下参数配置名为“working\_hours”的时间段。

名称	working_hours
类型	周期时间段
开始时间	09:00:00
结束时间	17:00:00
每周生效时间	星期一、星期二、星期三、星期四、星期五

- c. 单击“确定”。

4. 创建名称为 off\_hours 的时间段，该时间段为非工作时间，对应双休日全天（00:00:00 – 23:59:59）、工作日的 00:00:00 – 08:59:59 以及工作日的 17:01:00 – 23:59:59。

- a. 选择“对象 > 时间段”。
- b. 单击“新建”，按如下参数配置名为“off\_hours”的时间段。

名称	off_hours
类型	周期时间段
开始时间	00:00:00
结束时间	23:59:59
每周生效时间	星期六、星期日

- c. 向“off\_hours”添加时间段成员（工作日的 00:00:00 – 08:59:59），按如下参数进行配置。

类型	周期时间段
开始时间	00:00:00
结束时间	08:59:59
每周生效时间	星期一、星期二、星期三、星期四、星期五

- d. 向“off\_hours”添加时间段成员（工作日的 17:01:00 – 23:59:59），按如下参数进行配置。

类型	周期时间段
开始时间	17:01:00
结束时间	23:59:59
每周生效时间	星期一、星期二、星期三、星期四、星期五

- e. 单击“确定”。

5. 配置安全策略。

- a. 选择“策略 > 安全策略”。
- b. 单击“新建”，按如下参数配置名为“policy\_sec\_research\_work”的安全策略，通过引用用户、时间段和应用行为控制配置文件，用来控制研发员工在工作时间段的应用行为。

名称	policy_sec_research_work
源安全区域	trust
目的安全区域	untrust
用户	/default/research
时间段	working_hours

动作	permit
内容安全	
应用行为控制	profile_app_research_work

c. 单击“确定”。

d. 参考上述步骤，按如下参数配置名称为“policy\_sec\_research\_rest”安全策略。此策略通过引用用户、时间段和应用行为控制配置文件，用来控制研发员工在非工作时间段的应用行为。

名称	policy_sec_research_rest
源安全区域	trust
目的安全区域	untrust
用户	/default/research
时间段	off_hours
动作	permit
内容安全	
应用行为控制	profile_app_research_rest

e. 参考上述步骤，按如下参数配置名称为“policy\_sec\_marketing”安全策略。此策略通过引用用户和应用行为控制配置文件，用来控制市场员工的应用行为。

名称	policy_sec_marketing
源安全区域	trust
目的安全区域	untrust
用户	/default/marketing
动作	permit
内容安全	
应用行为控制	profile_app_marketing

6. 单击界面右上角的“保存”，在弹出的对话框中单击“确定”。

## 结果验证

配置完成后，分别在研发员工和市场员工的 PC 上进行 HTTP 和 FTP 权限的验证，如果符合 HTTP 和 FTP 权限控制的需求，则表示应用行为控制配置文件和安全策略的配置成功，否则请检查应用行为控制配置文件和安全策略的配置。

## 配置脚本

NGFW 的配置脚本:

```
#
time-range off_hours
  period-range 00:00:00 to 23:59:59 off-day
  period-range 00:00:00 to 08:59:59 working-day
  period-range 17:01:00 to 23:59:59 working-day
time-range working_hours
  period-range 09:00:00 to 17:00:00 working-day
#
sysname NGFW
#
interface GigabitEthernet1/0/1
  ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/3
  ip address 10.3.1.1 255.255.255.0
#
firewall zone trust
  add interface GigabitEthernet1/0/1
#
firewall zone untrust
  add interface GigabitEthernet1/0/3
#
profile type app-control name profile_app_research_work
  http-control post action deny
  http-control proxy action deny
  http-control web-browse action deny
  ftp-control file delete action deny
  http-control file direction upload action deny
  http-control file direction download action deny
  ftp-control file direction upload action deny
  ftp-control file direction download action deny

profile type app-control name profile_app_research_rest
  http-control post action deny
  ftp-control file delete action deny
  http-control file direction upload action deny
  ftp-control file direction upload action deny
  ftp-control file direction download action deny
```

```

profile type app-control name profile_app_marketing
  ftp-control file direction upload block-size 102400
  ftp-control file direction download block-size 102400
#
security-policy
  rule name policy_sec_research_work
    source-zone trust
    destination-zone untrust
    user /default/research
    time-range working_hours
    profile app-control profile_app_research_work
    action permit
  rule name policy_sec_research_rest
    source-zone trust
    destination-zone untrust
    user /default/research
    time-range off_hours
    profile app-control profile_app_research_rest
    action permit
  rule name policy_sec_marketing
    source-zone untrust
    destination-zone trust
    user /default/marketing
    profile app-control profile_app_marketing
    action permit
#
return

```

## HCIE-Security 模拟面试问题及面试建议

1. 在 NGFW 上能够做哪些应用行为控制？