

# HCIE-Security 备考指南

## 反病毒



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 反病毒需要掌握的知识点.....	1
反病毒简介.....	1
反病毒原理描述.....	1
使用限制和注意事项.....	5
反病毒应用场景.....	5
配置的反病毒特性没有生效.....	6
现象描述.....	6
可能原因.....	6
处理步骤.....	7
反病毒 FAQ.....	8
举例：配置反病毒.....	8
HCIE-Security 模拟面试问题及面试建议.....	14

## HCIE-Security 反病毒需要掌握的知识点

- 了解计算机病毒基础知识
- 掌握病毒特征及常用检测工具
- 熟悉网关防病毒主要技术
- 熟练掌握网关防病毒技术的应用

## 反病毒简介

介绍反病毒特性的定义和目的。

### 定义

病毒是一种恶意代码，可感染或附着在应用程序或文件中，一般通过邮件或文件共享等协议进行传播，威胁用户主机和网络的安全。有些病毒会耗尽主机资源、占用网络带宽，有些病毒会控制主机权限、窃取用户数据，有些病毒甚至会对主机硬件造成破坏。

反病毒是一种安全机制，它可以通过识别和处理病毒文件来保证网络安全，避免由病毒文件而引起的数据破坏、权限更改和系统崩溃等情况的发生。

### 目的

随着网络的不断发展和应用程序的日新月异，企业用户越来越频繁地开始在网络上传输和共享文件，随之而来的病毒威胁也越来越大。企业只有拒病毒于网络之外，才能保证数据的安全，系统的稳定。因此，保证计算机和网络系统免受病毒的侵害，让系统正常运行便成为企业所面临的一个重要问题。

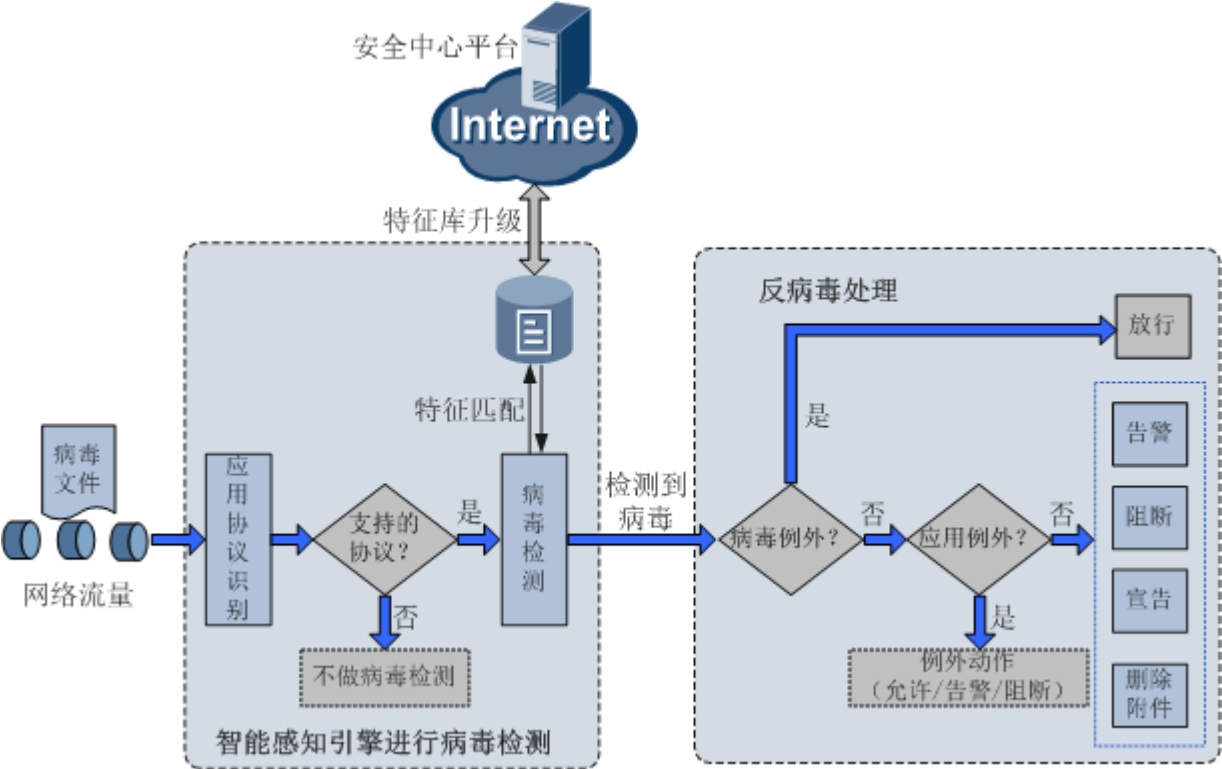
反病毒功能可以凭借庞大且不断更新的病毒特征库有效地保护网络安全，防止病毒文件侵害系统数据。将病毒检测设备部署在企业网的入口，可以真正将病毒抵御于网络之外，为企业网络提供了一个坚固的保护层。

## 反病毒原理描述

介绍反病毒特性的实现原理和处理流程。

NGFW 利用专业的智能感知引擎和不断更新的病毒特征库实现对病毒文件的检测和处理，其工作原理如[图 1](#)所示。

图 1 反病毒工作原理



智能感知引擎进行病毒检测

NGFW 的病毒检测是依靠智能感知引擎来进行的。流量进入智能感知引擎后：

1. 首先智能感知引擎对流量进行深层分析，识别出流量对应的协议类型和文件传输的方向。
2. 判断文件传输所使用的协议和文件传输的方向是否支持病毒检测。

NGFW 支持对使用以下协议传输的文件进行病毒检测：

- FTP（File Transfer Protocol）：文件传输协议
- HTTP（Hypertext Transfer Protocol）：超文本传输协议
- POP3（Post Office Protocol - Version 3）：邮局协议的第 3 个版本
- SMTP（Simple Mail Transfer Protocol）：简单邮件传输协议
- IMAP（Internet Message Access Protocol）：因特网信息访问协议
- NFS（Network File System）：网络文件系统
- SMB（Server Message Block）：文件共享服务器

NGFW 支持对不同传输方向上的文件进行病毒检测。

- 上传：指客户端向服务器发送文件。
- 下载：指服务器向客户端发送文件。

#### 说明：

由于协议的连接请求均由客户端发起，为了使连接可以成功建立，用户在配置安全策略时需要确保将源区域设置为客户端所在的安全区域、将目的区域设置为服务器所在的安全区域。

举例 1：Trust 区域的用户需要从 Untrust 区域的 FTP 服务器下载文件，此时需要在安全策略配置界面中将 Trust 区域设置为源安全区域，Untrust 区域设置为目的安全区域，在反病毒配置界面中选择 FTP 协议的检测方向为下载。

举例 2：Trust 区域的用户需要向 DMZ 区域的 SMTP 服务器上传邮件，此时需要在安全策略配置界面中将 Trust 区域设置为源安全区域，DMZ 区域设置为目的安全区域，在反病毒配置界面中选择 SMTP 协议的检测方向为上传。

### 3. 病毒检测。

智能感知引擎对符合病毒检测的文件进行特征提取，提取后的特征与病毒特征库中的特征进行匹配。如果匹配，则认为该文件为病毒文件，并按照配置文件中的响应动作进行处理。如果不匹配，则允许该文件通过。

病毒特征库是由华为公司通过分析各种常见病毒特征而形成的。该特征库对各种常见的病毒特征进行了定义，同时为每种病毒特征都分配了一个唯一的病毒 ID。当设备加载病毒特征库后，即可识别出特征库里已经定义过的病毒。同时，为了能够及时识别出最新的病毒，设备上的病毒特征库需要不断地从安全中心平台（[sec.huawei.com](http://sec.huawei.com)）进行升级。

#### 说明：

病毒特征库的升级服务需要购买相关的 License 后才能正常使用。

## 反病毒处理

当 NGFW 检测出传输文件为病毒文件时，需要进行如下处理：

1. 判断该病毒文件是否命中病毒例外。如果是病毒例外，则允许该文件通过。

病毒例外，即病毒白名单。为了避免由于系统误报等原因造成文件传输失败等情况的发生，当用户认为已检测到的某个病毒为误报时，可以将该对应的病毒 ID 添加到病毒例外，使该病毒规则失效。如果检测结果命中了病毒例外，则对该文件的响应动作即为放行。

2. 如果不是病毒例外，则判断该病毒文件是否命中应用例外。如果是应用例外，则按照应用例外的响应动作（放行、告警和阻断）进行处理。

应用例外可以为应用配置不同于协议的响应动作。应用承载于协议之上，同一协议上可以承载多种应用。例如，HTTP 协议上可以承载 163.com 的应用，也可以承载 yahoo.com 的应用。

由于应用和协议之间存在着这样的关系，在配置响应动作时也有如下规定：

- 如果只配置协议的响应动作，则协议上承载的所有应用都继承协议的响应动作。
- 如果协议和应用都配置了响应动作，则以应用的响应动作为准。

例如，HTTP 协议上承载了“163.com”和“yahoo.com”两种应用：

- 如果只配置了 HTTP 协议的响应动作为“阻断”，则“163.com”和“yahoo.com”的响应动作也都继承为“阻断”。
- 如果用户希望对“163.com”这个应用做区分处理，则可以将“163.com”添加为“应用例外”，其响应动作为“告警”。此时，“yahoo.com”的响应动作仍然继承 HTTP 协议的响应动作“阻断”，而“163.com”的响应动作将使用应用例外的响应动作“告警”。

3. 如果病毒文件既没命中病毒例外，也没命中应用例外，则按照配置文件中配置的协议和传输方向对应的响应动作进行处理。

NGFW 对不同协议在不同的文件传输方向上支持不同的响应动作，如下所示。

协议	传输方向	响应动作	说明
HTTP	上传/下载	告警/阻断，默认为阻断。	<ul style="list-style-type: none"> <li>• 告警：允许病毒文件通过，同时生成病毒日志。</li> <li>• 阻断：禁止病毒文件通过，同时生成病毒日志。</li> <li>• 宣告：对于携带病毒的邮件文件，设备允许该文件通过，但会在邮件正文中添加检测到病毒的提示信息，同时生成病毒日志。宣告动作仅对 SMTP 协议和 POP3 协议生效。</li> </ul>
FTP	上传/下载	告警/阻断，默认为阻断。	
NFS	上传/下载	告警	
SMB	上传/下载	告警/阻断，默认为阻断。	
SMTP	上传	告警/宣告/删除附件，默认为告警。	
POP3	下载	告警/宣告/删除附件，默认	

协议	传输方向	响应动作	说明
		为告警。	<ul style="list-style-type: none"> <li>删除附件：对于携带病毒的邮件文件，设备允许该文件通过，但设备会删除邮件中的附件内容并在邮件正文中添加宣告，同时生成病毒日志。删除附件动作仅对 SMTP 协议和 POP3 协议生效。</li> </ul>
IMAP	上传/下载	告警	

## 使用限制和注意事项

配置反病毒特性前请先阅读使用限制和注意事项。

- 反病毒功能和特征库的升级需要 License 支持。License 加载前，反病毒功能可配置，但不生效。License 加载完成后，需要手动加载 AV 特征库，才能正常使用反病毒功能。License 过期后，用户可以继续使用反病毒功能，但不能获取最新的反病毒特征库。为了保护网络安全，推荐继续购买 License。
- 反病毒特征库更新频繁，为保证反病毒功能的有效性，推荐定期升级反病毒特征库，具体操作请参见[升级中心](#)。
- 在报文来回路径不一致的组网环境中，针对 SMTP 和 POP3 协议的反病毒功能不可用。
- 在 IPv6 组网中，针对 IMAP、SMTP 和 POP3 协议的反病毒功能不可用。
- 不支持针对断点续传文件的反病毒检测。

## 反病毒应用场景

介绍反病毒特性的应用场景。

### 应用环境

在以下场合中，通常利用反病毒特性来保证网络安全：

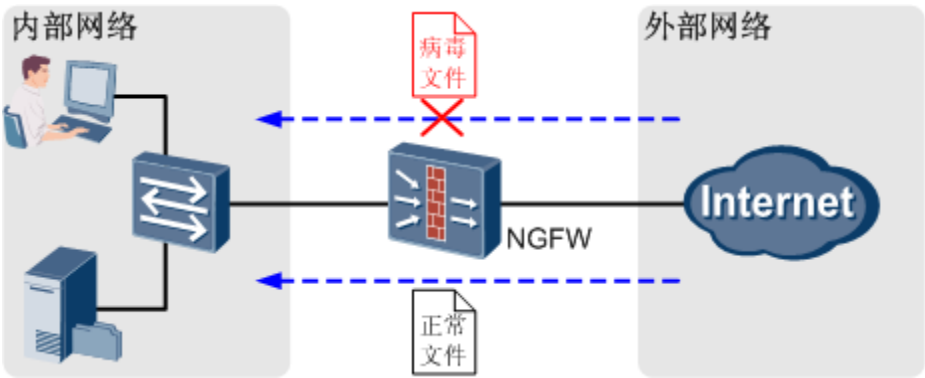
- 内网用户可以访问外网，且经常需要从外网下载文件。
- 内网部署的服务器经常接收外网用户上传的文件。

### 典型应用

如[图 1](#)所示，NGFW 作为网关设备隔离内、外网，内网包括用户 PC 和服务器。内网用户可以从外网下载文件，外网用户可以上传文件到内网服务器。为了保证内网用户和服务器接收文件的安全，需要在 NGFW 上配置反病

毒功能。

图 1 反病毒典型应用场景



在 NGFW 上配置反病毒功能后，正常文件可以顺利进入内部网络，包含病毒的文件则会被检测出来，并被采取阻断或告警等手段进行干预。

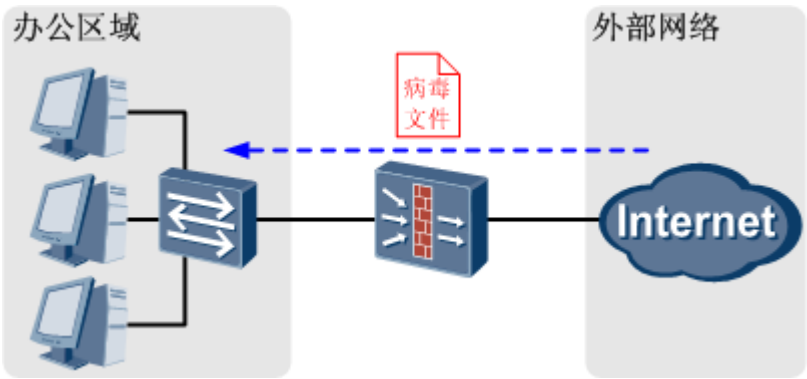
## 配置的反病毒特性没有生效

介绍配置反病毒功能后仍有病毒文件进入受保护网络时的故障排查方法。

### 现象描述

如图 1 所示，某公司在网络边界处部署了 NGFW 作为安全网关。NGFW 提供了反病毒功能，用于防止病毒文件进入内网、破坏网络安全。

图 1 网络环境示意图



实际使用中，办公区域的 PC1（10.3.0.2）在从外网收取邮件时，PC1 上的系统安全软件提示该邮件中的附件携带病毒，病毒 ID 为 8000。

### 可能原因

请分别按以下三种情况逐一排查可能原因：



- [原因一：NGFW 上配置的安全策略配置错误（没有引用反病毒配置文件）。](#)
- [原因二：NGFW 上的反病毒配置文件配置错误。](#)
- [原因三：NGFW 的病毒特征库版本较旧。](#)

## 处理步骤

### 原因一：NGFW 上配置的安全策略配置错误（没有引用反病毒配置文件）。

1. 找到 PC1 收取邮件时命中的安全策略。

选择“监控 > 日志 > 策略命中日志”。在“高级查询”中根据“开始时间”、“结束时间”、“目的地址”等条件查询 PC1 命中的安全策略。

2. 检查 PC1 命中的安全策略是否配置引用反病毒配置文件。

如果 PC1 命中的安全策略未引用反病毒配置文件，请创建反病毒配置文件，并在安全策略中引用。

如果已引用反病毒配置文件，请参照[原因二：NGFW 上的反病毒配置文件配置错误。](#)，检查该反病毒配置文件的配置是否正确。

### 原因二：NGFW 上的反病毒配置文件配置错误。

3. 选择“对象 > 安全配置文件 > 反病毒”，找到安全策略所引用的配置文件。

4. 检查反病毒配置文件的动作。

如果“邮件协议”的动作为“告警”，NGFW 将不能阻断病毒文件，请修改为“删除附件”。

5. 检查反病毒配置文件是否配置了应用例外。

如果反病毒配置文件中配置了应用例外，请确认 PC1 收取邮件的应用否属于该应用，如果属于该应用，请删除该应用例外。

6. 检查反病毒配置文件是否配置了病毒例外。

如果反病毒配置文件中配置了病毒例外，且该病毒的 ID 和 PC1 上的系统安全软件检测到的病毒 ID（8000）相同，请根据实际情况确认该病毒是否为真正的病毒，如果需要阻断该包含该病毒的文件，请删除该病毒例外。

### 原因三：NGFW 的病毒特征库版本较旧。

选择“系统 > 升级中心”，查看“反病毒特征库”的当前版本是否为最新版本。

如果当前版本不是最新版本，请进行版本升级。

如果以上原因均已排查无误，问题仍然没有解决，请联系技术支持工程师处理。

## 反病毒 FAQ

反病毒特性常见问题解答。

### 反病毒特性是否需要 License 支持？

需要。

反病毒功能和特征库的升级需要 License 支持。只有获取了 License，才能使用反病毒功能和升级反病毒特征库。

License 过期后，用户只能使用设备已有的反病毒功能，不能获取最新的反病毒特征库。

### 反病毒特性是否可以检测压缩文件？

可以检测 zip、gz 和 tar 类型的压缩文件，支持检测的最大压缩层数为 3 层。

### NGFW 提供的反病毒特性和用户主机上的防病毒软件什么关系？

NGFW 提供的反病毒特性和用户主机上的防病毒软件在功能上是互补和协作的关系。由于部署位置和特征库的不同，两者可以同时使用，更有力的保障用户主机和网络的安全。

## 举例：配置反病毒

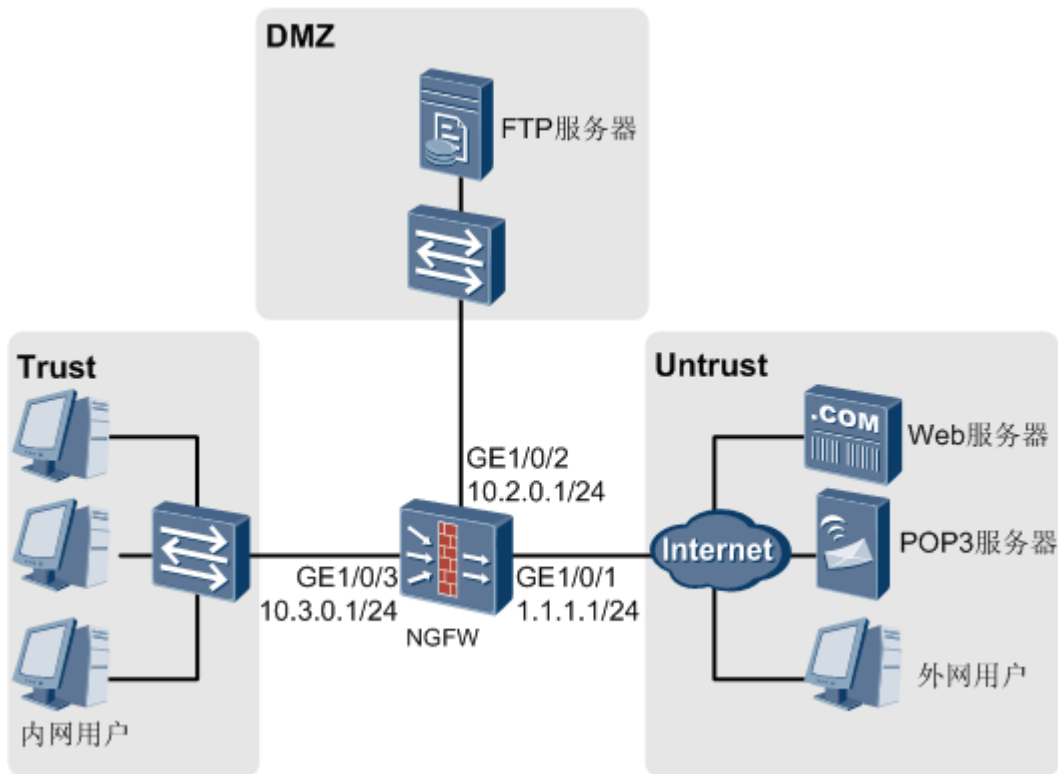
在企业网关设备上应用反病毒特性，保护内部网络用户和服务器免受病毒威胁。

## 组网需求

某公司在网络边界处部署了 NGFW 作为安全网关。内网用户需要通过 Web 服务器和 POP3 服务器下载文件和邮件，内网 FTP 服务器需要接收外网用户上传的文件。公司利用 NGFW 提供的反病毒功能阻止病毒文件在这些过程中进入受保护网络，保障内网用户和服务器的安全。网络环境如图 1 所示。

其中，由于公司使用 Netease 邮箱作为工作邮箱，为了保证工作邮件的正常收发，需要放行 Netease 邮箱的所有邮件。另外，内网用户在通过 Web 服务器下载某重要软件时失败，排查发现该软件因被 NGFW 判定为病毒而被阻断（病毒 ID 为 8000），考虑到该软件的重要性和对该软件来源的信任，管理员决定临时放行该类病毒文件，以使用户可以成功下载该软件。

图 1 配置反病毒组网图



## 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. 配置两个反病毒配置文件，一个反病毒配置文件针对 HTTP 和 POP3 协议设置匹配条件和响应动作，并在该配置文件中配置 Netease 邮箱的应用例外和病毒 ID 为 8000 的病毒例外，另外一个反病毒配置文件针对 FTP 协议设置匹配条件和响应动作。
3. 配置安全策略，在 Trust 到 Untrust 和 DMZ 到 Untrust 方向分别引用反病毒配置文件，实现组网需求。

## 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 GE1/0/2 接口。

安全区域	dmz
IPv4	
IP 地址	10.2.0.1/24

- e. 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	10.3.0.1/24

2. 配置反病毒配置文件。

- a. 选择“对象 > 安全配置文件 > 反病毒”。
- b. 单击“新建”，按下图完成针对 HTTP 和 POP3 协议的配置。

名称: AV\_http\_pop3

描述: http\_pop3

抓包: ☐ 启用 检测到病毒后, 系统会抓取包含病毒的数据包。您可以在日志中查看数据包内容。

高危特征检测: ☐ 启用

协议	文件传输协议		邮件协议			共享协议	
	HTTP	FTP	SMTP	POP3	IMAP(?)	NFS(?)	SMB(?)
上传	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
下载	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
动作	阻断	阻断	告警	删除附件	告警	告警	阻断

应用例外

请输入或选择应用名称: [下拉] [添加] [删除]

名称	动作
<input checked="" type="checkbox"/> Netease邮箱网页版	允许

共 1 条

病毒例外

请输入病毒ID: [下拉] [添加] [删除]

ID	名称
<input checked="" type="checkbox"/> 8000	Trojan.Win32.Scar.34

没有记录

应用例外是针对应用层服务做检测, 如果用户所选应用承载于上述任 加入“病毒例外”的病毒不受反病毒规则的影响。您可以从日志信息

确定 取消

- c. 单击“确定”。
- d. 参考上述步骤按如下参数完成针对 FTP 协议的配置。

名称: AV\_ftp

描述: ftp

抓包: ☐ 启用 检测到病毒后, 系统会抓取包含病毒的数据包。您可以在日志中查看数据包内容。

高危特征检测: ☐ 启用

协议	文件传输协议		邮件协议			共享协议	
	HTTP	FTP	SMTP	POP3	IMAP(?)	NFS(?)	SMB(?)
上传	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
下载	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
动作	阻断	阻断	告警	告警	告警	告警	阻断

3. 配置内网用户到外网服务器方向（Trust 到 Untrust 方向）的安全策略。

- a. 选择“策略 > 安全策略 > 安全策略”。
- b. 单击“新建”。
- c. 在“新建安全策略”中应用反病毒配置文件。参数配置如下。

名称	policy_av_1
描述	Intranet-User

源安全区域	trust
目的安全区域	untrust
动作	permit
内容安全	
反病毒	AV_http_pop3

d. 单击“确定”。


- 配置外网用户到内网服务器方向（Untrust 到 DMZ 方向）的安全策略。

参照内网用户到外网服务器方向安全策略的配置方法，完成安全策略的配置。参数配置如下。

名称	policy_av_2
描述	Intranet-Server
源安全区域	untrust
目的安全区域	dmz
动作	permit
内容安全	
反病毒	AV_ftp

- 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，可以进入“监控 > 日志 > 威胁日志”查看威胁类型为“病毒”的威胁日志。单击可以查看日志的详细信息。

## 配置脚本

NGFW 的配置脚本：

```
#
sysname NGFW
#
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 10.3.1.1 255.255.255.0
#
firewall zone trust
add interface GigabitEthernet1/0/3
#
firewall zone untrust
add interface GigabitEthernet1/0/1
#
firewall zone dmz
add interface GigabitEthernet1/0/2
#
profile type av name default
profile type av name AV_http_pop3
description http-pop3
http-detect direction download
undo ftp-detect
undo smtp-detect
pop3-detect action delete-attachment
undo imap-detect
undo nfs-detect
undo smb-detect
exception application name Yahoo_WebMail action allow
exception av-signature-id 8000
profile type av name AV_ftp
description ftp
undo http-detect
ftp-detect direction upload
undo smtp-detect
undo pop3-detect
undo imap-detect
undo nfs-detect
undo smb-detect
#
security-policy
rule name policy_av_1
description Intranet-User
source-zone trust
destination-zone untrust
profile av AV_http_pop3

```

```
    action permit
rule name policy_av_2
    description Intranet-Server
    source-zone untrust
    destination-zone dmz
    profile av AV_ftp
    action permit
#
return
```

## HCIE-Security 模拟面试问题及面试建议

1. NGFW 反病毒支持哪些协议？