

HCNP-Security-CSSN

实验指导手册

版本:3.0



华为技术有限公司

更多资料获取：<http://learning.huawei.com/cr>

版权所有 © 华为技术有限公司 2017。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI 和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址：	深圳市龙岗区坂田华为总部办公楼	邮编：518129
网址：	http://e.huawei.com	



华为认证体系介绍

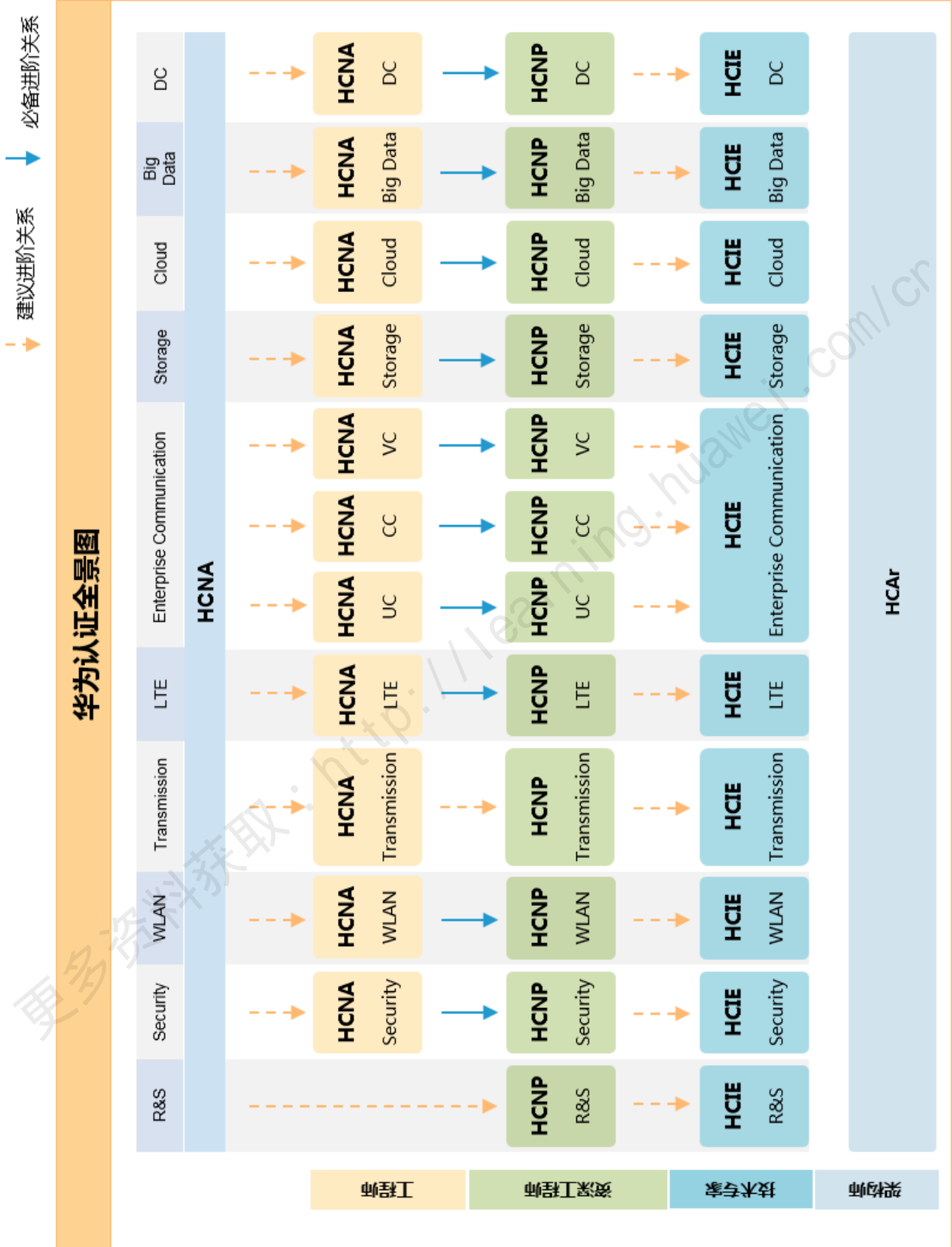
依托华为公司雄厚的技术实力和专业的培训体系，华为认证考虑到不同客户对网络安全技术不同层次的需求，致力于为客户提供实战性、专业化的技术认证。

根据网络安全技术的特点和客户不同层次的需求，华为认证为客户提供面向各个方向的四级认证体系。

HCNP-Security (Huawei Certified Network Professional-Security, 华为认证网络高级工程师安全方向) 主要面向华为公司办事处、代表处一线工程师，以及其他希望学习华为网络安全产品和网络安全技术的人士。HCNP-Security认证涵盖华为网络安全、内容安全和终端安全的内容。

华为认证协助您打开行业之窗，开启改变之门，屹立在网络安全世界的潮头浪尖！

更多资料获取：<http://learning.huawei.com/cn>



前言

简介

本书为 HCNP-Security-CSSN 认证培训教程，适用于准备参加 HCNP-Security-CSSN 考试的学员或者希望了解内容安全过滤，NIP 入侵防御，防病毒攻击，防火墙防单包及流量型攻击等相关安全技术的读者。

内容描述

本实验指导书共包含 5 个实验，从内容安全过滤开始，逐一介绍了 NIP 入侵防御、服务器防病毒攻击、用户防病毒攻击、防火墙单包攻击防范、防火墙流量型攻击防范的配置实践。

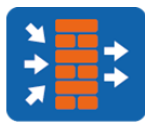
- 实验一内容安全过滤综合实验，包含文件过滤、邮件过滤、内容过滤、应用行为控制、URL 过滤，通过配置防火墙安全文件，了解防火墙内容安全的功能及配置。
- 实验二为 NIP 入侵阻断实验，通过 NIP 直路部署，了解 NIP 的工作原理及配置，以及如何查看攻击防御记录。
- 实验三为应用服务器防病毒攻击实验，通过部署针对邮件应用服务器的反病毒策略，保护内网服务器不被外网病毒攻击。
- 实验四为用户防病毒攻击实验，通过部署针对客户端的反病毒策略，保护内网用户不被外网病毒攻击。
- 实验五为防火墙通用防范实验（单包攻击防范），通过在防火墙上部署单包攻击防范，了解防火墙防范单包攻击的原理及配置。
- 实验五为防火墙通用防范实验（流量型攻击防范），通过在防火墙上部署 Anti-DDoS 策略，了解防火墙防范 DDoS 攻击的原理及配置。

读者知识背景

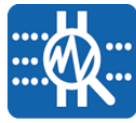
本课程为华为认证中级课程，为了更好地掌握本书内容，阅读本书的读者应首先具备以下基本条件：

- 具有基本的路由交换网络知识背景，同时熟悉华为交换设备，了解基本数通知识。

本书常用图标



防火墙



NIP产品



通用路由器



通用交换机



AP


 邮件服务器
(SMC)


Web服务器



FTP服务器



网络云2



通用服务器



PC



手机

实验环境说明

组网说明

本实验环境面向准备 HCNP-Security 考试的网络安全工程师。每套实验环境包括防火墙 3 台，交换机 4 台，路由器 3 台，服务器若干，主机若干。每套实验环境适用于 4 名学员同时上机操作。

设备介绍

为了满足 HCNP-Security 实验需要，建议每套实验环境采用以下配置：

设备名称、型号与版本的对应关系如下：

设备名称	设备型号	软件版本
USG防火墙	USG6530	5.160 (USG6500 V500R001C30SPC100)
交换机	S5700	5.130 (S5700 V200R003C00SPC300)
路由器	AR2200	5.160 (AR2200 V200R007C00SPC900)
Agile Controller服务器	Agile Controller	Agile Controller-Campus V100R002C10SPC400
AnyOffice配套服务器	AnyOffice	

准备实验环境

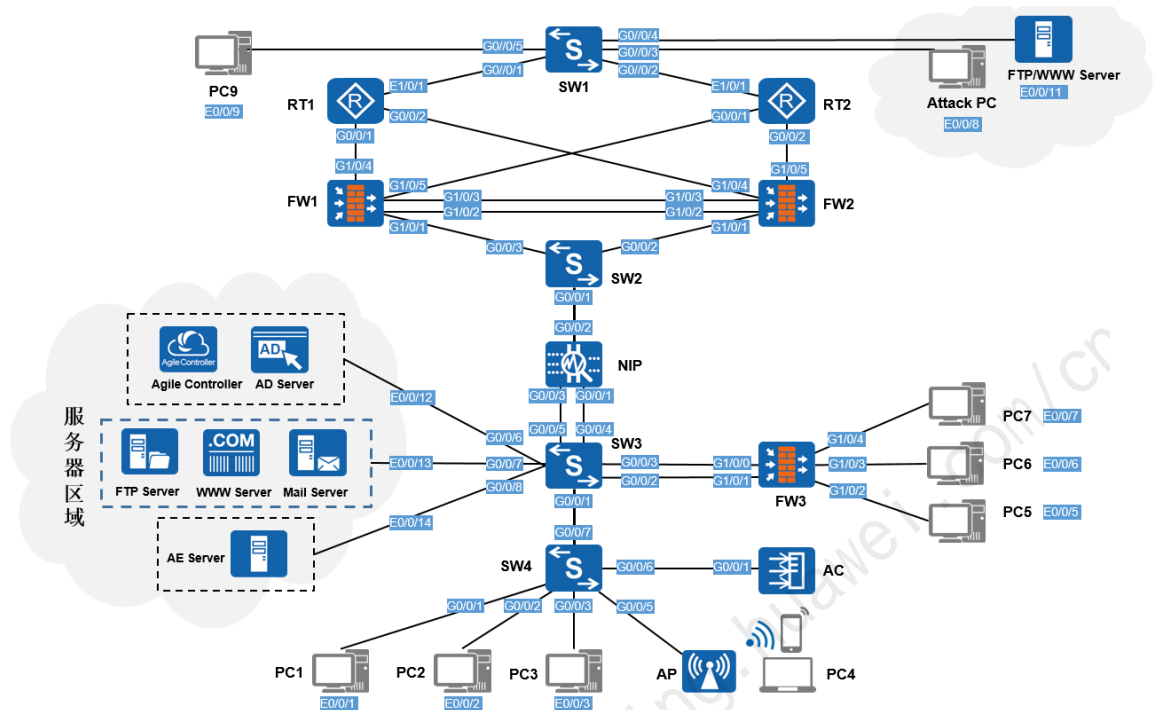
检查设备

实验开始之前请每组学员检查自己的实验设备是否齐全，实验清单如下。

设备名称	数量	备注
服务器群组 (HTTP/FTP/Mail/AC/SC/SM/Anyoffice)	各1台	
华为USG6370防火墙	3台	
华为S5700交换机	4台	
AP4030DN	1个	
虚拟主机	7台	

更多资料获取：<http://learning.huawei.com/cr>

实验拓扑



拓扑图组建说明：

本实验拓扑模拟了一个小型企业网络。FW1 与 FW2 部署为双机热备组网，作为企业边界设备控制出口流量。

在企业内部部署了终端用户和服务器资源，并有 NIP 设备监控网络入侵情况。

在企业内部可实现终端安全部署。

在 HCNP-Security v3.0 版本中的实验均在此拓扑中完成。

基础配置说明

实验开始前，需完成各设备的接口地址、安全区域及基本路由信息的相关配置。在后续的实验过程中，不再对以上基础信息配置进行说明。

主机登录信息：

名称	管理地址	账户
Server-AC	172.21.20.78/16	Administrator/Admin@123
Server-AD	172.21.20.72/16	Administrator/Auawei@123
Server-FTP	172.21.20.73/16	Administrator/Admin@123
Server-WWW	172.21.20.74/16	Administrator/Admin@123
Server-Mail	172.21.20.75/16	Administrator/Admin@123
Server-AE	172.21.20.76/16	Administrator/Admin@123
Server-FTP(INT)	172.21.20.80/16	Administrator/Admin@123
PC1	172.21.20.101/16	admin/Huawei123
PC2	172.21.20.102/16	admin/Huawei123
PC3	172.21.20.103/16	admin/Huawei123
PC4	172.21.20.104/16	admin/Huawei123
PC5	172.21.20.105/16	admin/Huawei 123
PC6	172.21.20.106/16	admin/Huawei 123
PC7	172.21.20.107/16	admin/Huawei 123
PC8 (Attack PC)	172.21.20.108/16	admin/Huawei 123
PC9	172.21.20.109/16	admin/Huawei 123

设备登录信息：

名称	管理口地址 (web/telnet)	账户
FW1	172.21.20.11/16	admin/Huawei@123
FW2	172.21.20.12/16	admin/Huawei@123
FW3	172.21.20.13/16	admin/Huawei@123
NIP	172.21.20.61/16	admin/Huawei@123
R1	172.21.20.21/16	Huawei@123
R2	172.21.20.22/16	Huawei@123
R3	172.21.20.23/16	Huawei@123
SW1	172.21.20.31/16	Huawei@123
SW2	172.21.20.32/16	Huawei@123
SW3	172.21.20.33/16	Huawei@123
SW4	172.21.20.34/16	Huawei@123
AP	172.21.20.51 /16	

防火墙数据规划：

名称	接口	安全区域	IP Address
FW1	G1/0/1	Trust	10.1.50.11/24
	G1/0/2	DMZ	10.1.61.11/24
	G1/0/3	DMZ	10.1.62.11/24
	G1/0/4	ISP1	10.1.71.11/24
	G1/0/5	ISP2	10.1.73.11/24
FW2	G1/0/1	Trust	10.1.50.12/24
	G1/0/2	DMZ	10.1.61.12/24
	G1/0/3	DMZ	10.1.62.12/24
	G1/0/4	ISP1	10.1.72.12/24
	G1/0/5	ISP2	10.1.74.12/24
FW3	G1/0/0	Trust	10.1.20.13/24
	G1/0/1	Untrust	10.1.21.13/24
	G1/0/2		10.1.25.13/24
	G1/0/3		10.1.26.13/24
	G1/0/4		10.1.27.13/24

路由器数据规划：

名称	接口	IP Address
R1	G0/0/1	10.1.71.21/24
	G0/0/2	10.1.72.21/24
	E1/0/1	10.1.81.21/24
R2	G0/0/1	10.1.73.22/24
	G0/0/2	10.1.74.22/24
	E1/0/1	10.1.82.22/24

交换机数据规划：

名称	接口	IP Address
SW1	G0/0/1	10.1.81.31/24
	G0/0/2	10.1.82.31/24
	G0/0/3	10.1.93.31/24
	G0/0/4	10.1.92.31/24
	G0/0/5	10.1.91.31/24
SW2	G0/0/1	N/A
	G0/0/2	N/A
	G0/0/3	N/A
SW3	G0/0/1	10.1.10.33/24
	G0/0/2	10.1.21.33/24
	G0/0/3	10.1.20.33/24
	G0/0/4	10.1.40.33/24
	G0/0/5	10.1.50.33/24
	G0/0/6	10.1.31.33/24
	G0/0/7	10.1.32.33/24
	G0/0/8	10.1.33.33/24
SW4	G0/0/1	10.1.11.34/24
	G0/0/2	10.1.12.34/24
	G0/0/3	
	G0/0/5	
	G0/0/6	10.1.13.34/24
	G0/0/7	10.1.10.34/24



设备预配脚本

本实验手册基于综合拓扑完成。各设备均包含预配信息，如果重置了环境，请按如下预配信息设置基本信息。设备密码均为 Huawei@123。

实验验证文件

序号	实验	验证文件
1	文件过滤实验	test.exe
2	邮件过滤实验	test.mp4
3	应用行为控制实验	test.mp4
4	应用服务器防病毒攻击实验	eicar_com.zip
5	内网用户防病毒攻击实验	eicar_com.zip

更多资料获取：<http://learning.huawei.com/cn>



目录

前 言	iv
简介	iv
内容描述	iv
读者知识背景	iv
本书常用图标	v
实验环境说明	v
准备实验环境	vi
1 实验一：内容安全过滤综合实验	xv
1.1 实验介绍	xv
1.1.1 关于本实验	xv
1.1.2 实验目的	xv
1.1.3 实验拓扑图	xv
1.1.4 前提条件	xvi
1.1.5 实验规划	xvi
1.1.6 实验任务列表	xviii
1.2 实验任务配置	xviii
1.2.1 配置思路	xviii
1.2.2 任务一：文件过滤	xviii
1.2.3 任务二：内容过滤	xxiii
1.2.4 任务三：邮件过滤	xxv
1.2.5 任务四：应用行为控制	xxvii
1.2.6 任务五：URL 过滤	xxix
1.3 配置参考	xxxii
2 NIP 入侵阻断实验	35
2.1 实验介绍	35
2.1.1 关于本实验	35
2.1.2 实验目的	35
2.1.3 实验拓扑图	35
2.1.4 前提条件	36



2.1.5 实验任务列表	36
2.2 实验任务配置	36
2.2.1 配置思路	36
2.2.2 配置步骤	36
3 应用服务器防病毒攻击实验	42
3.1 实验介绍	42
3.1.1 关于本实验	42
3.1.2 实验目的	42
3.1.3 实验拓扑图	42
3.1.4 前提条件	43
3.1.5 实验规划	43
3.1.6 实验任务列表	43
3.2 实验任务配置	44
3.2.1 配置思路	44
3.2.2 配置步骤	44
3.3 结果验证	47
3.4 配置参考	49
3.4.1 FW 的配置	49
4 内容用户防病毒攻击实验	51
4.1 实验介绍	51
4.1.1 关于本实验	51
4.1.2 实验目的	51
4.1.3 实验拓扑图	51
4.1.5 前提条件	52
4.1.6 实验规划	52
4.1.7 实验任务列表	52
4.2 实验任务配置	53
4.2.1 配置思路	53
4.2.2 配置步骤	53
4.3 结果验证	56
4.4 配置参考	56



4.4.1 FW 1 的配置	56
5 防火墙单包攻击防范实验	58
5.1 实验介绍	58
5.1.1 关于本实验	58
5.1.2 实验目的	58
5.1.3 实验拓扑图	58
5.1.4 前提条件	58
5.1.5 实验任务列表	59
5.2 实验任务配置	59
5.2.1 配置步骤（任务一）	59
5.3 结果验证	60
5.3.1 查看防火墙的日志	60
5.4 配置参考	61
5.4.1 FW1 的配置	61
6 防火墙流量型攻击防范实验	62
6.1 实验介绍	62
6.1.1 关于本实验	62
6.1.2 实验目的	62
6.1.3 实验拓扑图	62
6.1.4 前提条件	62
6.1.5 实验任务列表	63
6.2 实验任务配置	63
6.2.1 配置步骤	63
6.3 结果验证	64
6.3.1 查看防火墙的日志	64
6.4 配置参考	65
6.4.1 FW1 的配置	65

1

实验一：内容安全过滤综合实验

1.1 实验介绍

1.1.1 关于本实验

某公司在网络边界处部署了 FW 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：

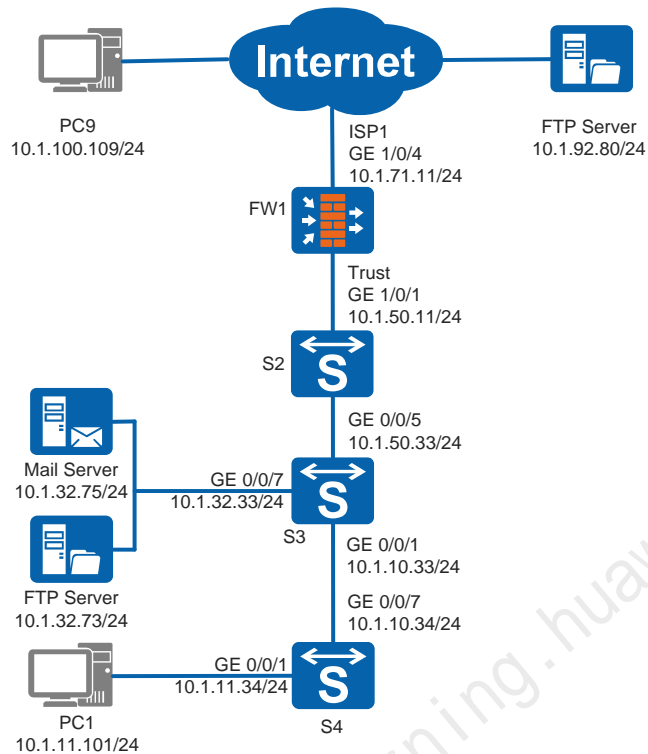
- 为了防止公司机密文件的泄露，禁止员工上传常见文档文件、代码文件（C、CPP、JAVA）以及压缩文件到 Internet 服务器；
- 为了降低病毒进入公司内部的风险，禁止员工从 Internet 下载可执行文件以及 Internet 用户上传可执行文件到内网服务器；
- 公司希望在保证网络正常使用的同时，防止内部员工泄露公司机密信息；
- 公司规定发送往外网或接收来自外网的邮件单个附件均不能超过 2M；
- 公司希望员工上传和下载的文件大小不能超过 2M；
- 外网网站 <http://10.1.92.80> 疑似有安全隐患，内网员工不能访问该网站且不能访问社交网络等网站。

1.1.2 实验目的

- 掌握文件、内容、邮件过滤以及应用行为控制的应用场景；
- 掌握文件、内容、邮件过滤的配置方法。

1.1.3 实验拓扑图

图1-1 内容安全过滤综合实验拓扑图



1.1.4 前提条件

1. 配置防火墙网络连接、IP 地址、接口安全区域。
2. 完成防火墙 FW1 和 FW2 的双机热备组网配置。
3. NAT 策略部署完成。

1.1.5 实验规划

表1-1 实验数据规划

项目	数据	说明
安全策略 to_Internet	名称: to_Internet 源安全区域: trust 目的安全区域: isp1 动作: 允许 文件过滤: profile_file_1 内容过滤: profile_data_1 邮件过滤: profile_mail_1 应用行为: profile_app_1	安全策略“to_Internet”的作用是允许公司员工访问 Internet。

安全策略 to_intra_server	名称: to_intra_server 源安全区域: isp1 目的安全区域: trust 目的地址: 10.1.32.0/24 动作: 允许 文件过滤: profile_file_2 邮件过滤: profile_mail_1	安全策略 “to_intra_server”的作用是允许外网用户访问内网服务器。
文件过滤 profile_file_1	名称: rule1 文件类型: 文档文件、代码文件、压缩文件 方向: 上传 动作: 阻断	禁止员工上传文档、开发和压缩文件到 Internet。
	名称: rule2 文件类型: 可执行文件 方向: 下载 动作: 阻断	禁止员工从 Internet 下载可执行文件。
文件过滤 profile_file_2	名称: rule1 文件类型: 可执行文件 方向: 上传 动作: 阻断	禁止 Internet 向内网服务器上传可执行文件
内容过滤 profile_data_1	名称: rule1 关键字: key1 应用: all 文件类型: all 方向: 上传 动作: 阻断	阻断关键字为 key1 的内容的上传。
邮件过滤 profile_mail_1	控制项: 垃圾邮件过滤 发送/接收附件大小限制: 2M	防止垃圾邮件并控制附件单个附件大小不超过 2M。
应用行为控制 profile_app_1	控制项: FTP 上传/下载阻断阈值 100M	文件超出 100M 会执行阻断

URL 过滤 Profile_URL_1	自定义 URL 分类，将 HTTP://10.1.92.80 网站设置为禁止访问。	禁止访问 http://10.1.92.80
-------------------------	---	---

1.1.6 实验任务列表

序号	任务	子任务	任务说明
1	内容安全过滤 配置文件	文件过滤	禁止员工上传常见文档文件、代码文件（C、CPP、JAVA）以及压缩文件到Internet服务器；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
		内容过滤	防止内部员工泄露公司机密信息
		邮件过滤	邮件发送接收单个附件均不能超过2M
		应用行为控制	上传和下载的文件大小不能超过100M
		URL过滤	禁止访问外网网站 http://10.1.92.80
2	安全策略	内网用户访问 Internet	配置安全策略并调用文件过滤、内容过滤、邮件过滤、应用行为控制以及URL过滤以满足需求
		外网用户访问 内网服务器	配置安全策略并调用文件过滤和邮件过滤以满足需求

1.2 实验任务配置

1.2.1 配置思路

1. 基本网络参数配置；
2. 网络地址转换配置。
3. 内容安全过滤文件配置；
4. 安全策略配置引用内容安全配置文件；

1.2.2 任务一：文件过滤

步骤 1 文件过滤配置文件。

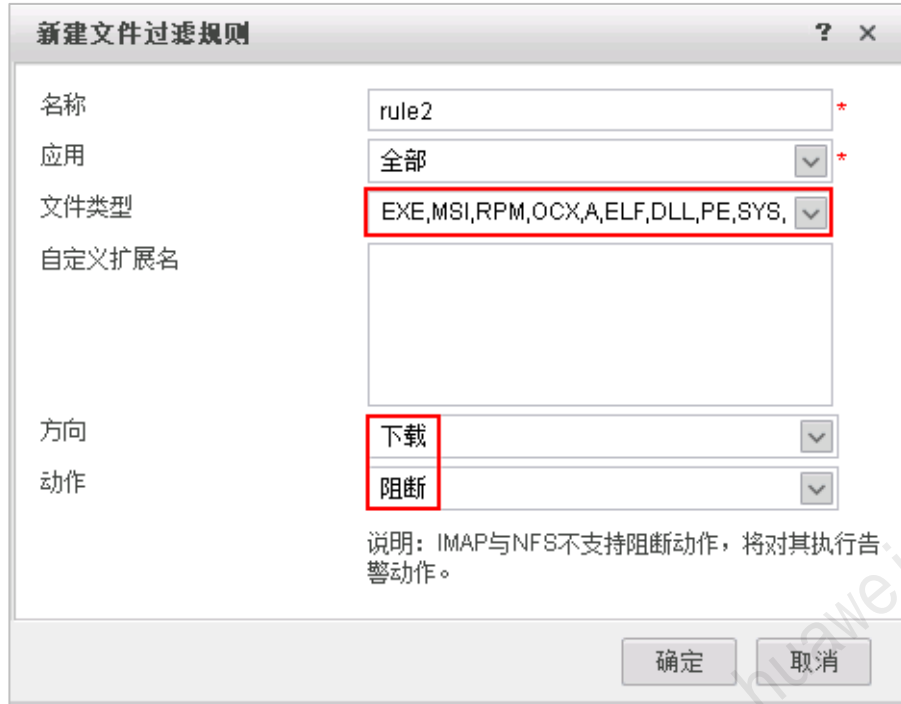
- 1) 选择“对象>安全配置文件>文件过滤>文件过滤配置文件”。在文件过滤规则菜单中，单击“新建”，新建文件过滤配置文件 profile_file_1，单击“新建”，新建文件过滤规则。



- a. 新建规则 1 阻断文档文件、代码文件、压缩文件的上传。



- b. 新建规则 2 阻断可执行文件下载



c. 点击“确定”。



2) 新建文件过滤配置文件“profile_file_2”。

a. 点击“新建”。



b. 新建规则 1 阻断可执行文件上传



新建文件过滤规则

名称 rule1 *

应用 全部 *

文件类型 EXE,MSI,RPM,OCX,A,ELF,DLL,PE,SYS

自定义扩展名

方向 上传

动作 阻断

说明：IMAP与NFS不支持阻断动作，将对其执行告警动作。

确定 取消

步骤 2 安全策略引用内容安全配置文件。

- 1) 选择“策略>安全策略”，单击新建安全策略“to_Internet”，用于允许内网用户访问外网，并引用文件过滤配置文件 profile_file_1。

新建安全策略

提示：新建时可以基于策略模板来快速定义您需要的策略。[选择策略模板]

名称	to_internet	*
描述		
策略组	-- NONE --	
源安全区域	trust	[修改]
目的安全区域	isp1	[修改]
源地址/地区	10.1.11.0/24	
目的地址/地区	请选择或输入地址	
用户	请选择或输入用户	[修改]
接入方式	请选择接入方式	
终端设备	请选择终端设备	
服务	请选择服务	
应用	请选择应用或应用组	[修改]
时间段	any	
动作	<input checked="" type="radio"/> 允许 <input type="radio"/> 禁止	

内容安全		
反病毒	-- NONE --	[配置]
入侵防御	-- NONE --	[配置]
URL过滤	-- NONE --	[配置]
文件过滤	profile_file_1	[配置]
内容过滤	-- NONE --	[配置]
应用行为控制	-- NONE --	[配置]
邮件过滤	-- NONE --	[配置]
APT防御	-- NONE --	[配置]

记录策略命中日志 启用

记录会话日志 启用

会话老化时间 <1-65535>秒

自定义长连接 启用

* <0-24000>小时

确定 取消

- 2) 新建安全策略“to_intra_server”，用于允许外网用户访问内部服务器，并引用文件过滤配置文件 profile_file_2。



步骤 3 提交配置。

步骤 4 结果验证。

- 内网用户 PC1 无法上传常见文档文件、代码文件（C、CPP、JAVA）以及压缩文件到 Internet 上的 FTP server；
- 内网用户 PC1 无法从 Internet 上的 FTP server 下载可执行文件；
- Internet 用户 PC9 不能上传可执行文件到内网 FTP 服务器；

1.2.3 任务二：内容过滤

步骤 1 内容过滤配置文件。

- 1) 选择“对象>关键字组>新建”，新建关键字组 key1。新建自定义关键字“公司违规信息”。

新建关键字

名称: 公司违规信息 *

描述:

匹配模式: 文本 正则表达式

文本: 违规信息 *

权重: 1 <1-255>

确定 取消

新建关键字组

名称: key1 *

描述:

关键字列表

+ 新建 - 删除

名称	描述	匹配模式	文本/正则表达式	权重<1-255>	编辑
自定义					
<input checked="" type="checkbox"/>	公司违规...	文本	违规信息	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

共 6 条

确定 取消

- 2) 新建内容过滤配置文件“profile_data_1”。新建内容过滤规则阻断内容匹配关键字 key1 的文件上传。

新建内容过滤配置文件

名称: profile_data_1 *

描述:

内容过滤规则

+ 新建 - 删除

名称	关键字组	应用	文件类型	方向	动作	告警阈值	阻断阈值	编辑	
<input type="checkbox"/>	rule	key1	全部	全部	上传	阻断	-	-	

步骤 2 安全策略引用内容安全配置文件。

- 1) 选择“策略>安全策略”，单击新建安全策略“to_Internet”，用于允许内网用户访问外网，并引用内容过滤配置文件 profile_data_1。



新建安全策略

提示：新建时可以基于策略模板来快速定义您需要的策略。[选择策略模板]

名称 to_internet *

描述

策略组 -- NONE --

源安全区域 trust 修改

目的安全区域 isp1 修改

源地址/地区 请选择或输入地址

目的地址/地区 请选择或输入地址

用户 请选择或输入用户 修改

接入方式 请选择接入方式

终端设备 请选择终端设备

服务 请选择服务

应用 请选择应用或应用组 修改

时间段 any

动作 允许 禁止

内容安全

反病毒	-- NONE --	配置
入侵防御	-- NONE --	配置
URL过滤	-- NONE --	配置
文件过滤	-- NONE --	配置
内容过滤	profile_data_1	配置
应用行为控制	-- NONE --	配置
邮件过滤	-- NONE --	配置
APT防御	-- NONE --	配置

记录策略命中日志 启用

记录会话日志 启用

会话老化时间 <1-65535>秒

自定义长连接 启用

168 *0-24000>小时

确定 取消

步骤 3 提交配置。

步骤 4 验证结果。

- 内部员工 PC1 无法上传包含关键字的公司文件到 Internet 上的 FTP server；

1.2.4 任务三：邮件过滤

步骤 1 邮件过滤配置文件。

- 1) 选择“对象 > 安全配置文件 > 邮件过滤”。新建邮件内容过滤文件，过滤垃圾邮件并阻止单个邮件附件大小超过 2M 的文件发送和接收。



步骤 2 安全策略引用内容安全配置文件。

- 1) 新建安全策略“to_intra_server”，用于允许外网用户访问内部服务器，并引用邮件过滤配置文件 profile_mail_1。



新建安全策略

提示: 新建时可以基于策略模板来快速定义您需要的策略。[选择策略模板]

名称 to_intra_server *

描述

策略组 -- NONE --

源安全区域 isp1 [修改]

目的安全区域 trust [修改]

源地址/地区 请选择或输入地址

目的地址/地区 请选择或输入地址

用户 请选择或输入用户 [修改]

接入方式 请选择接入方式

终端设备 请选择终端设备

服务 请选择服务

应用 请选择应用或应用组 [修改]

时间段 请选择时间段

动作 允许 禁止

内容安全

反病毒 -- NONE -- [配置]

入侵防御 -- NONE -- [配置]

URL过滤 -- NONE -- [配置]

文件过滤 -- NONE -- [配置]

内容过滤 -- NONE -- [配置]

应用行为控制 -- NONE -- [配置]

邮件过滤 profile_mail_1 [配置]

APT防御 -- NONE -- [配置]

记录策略命中日志 启用

记录会话日志 启用

会话老化时间 <1-65535>秒

自定义长连接 启用

168 *≤0-24000>小时

确定 取消

步骤 3 提交配置。

步骤 4 结果验证。

- PC9 不能发送单个附件超过 2M 的邮件到内网；
- PC1 发送超过 2M 附件的邮件，PC9 无法接收。

1.2.5 任务四：应用行为控制

步骤 1 应用行为控制配置文件。

- 1) 选择“对象 > 安全配置文件 > 应用行为控制”。新建应用行为控制配置文件，阻断 FTP 上传和下载大小超过 2M 的文件。



步骤 2 安全策略引用内容安全配置文件。

- 1) 选择“策略>安全策略”，单击新建安全策略“to_Internet”，用于允许内网用户访问外网，并引用内容安全配置文件。

新建安全策略

提示：新建时可以基于策略模板来快速定义您需要的策略。[选择策略模板]

名称 to_internet *

描述

策略组 -- NONE --

源安全区域 trust 修改

目的安全区域 isp1 修改

源地址/地区 请选择或输入地址

目的地址/地区 请选择或输入地址

用户 请选择或输入用户 修改

接入方式 请选择接入方式

终端设备 请选择终端设备

服务 请选择服务

应用 请选择应用或应用组 修改

时间段 any

动作 允许 禁止

内容安全

反病毒 -- NONE -- 配置

入侵防御 -- NONE -- 配置

URL过滤 -- NONE -- 配置

文件过滤 -- NONE -- 配置

内容过滤 -- NONE -- 配置

应用行为控制 profile_app_1 配置

邮件过滤 -- NONE -- 配置

APT防御 -- NONE -- 配置

记录策略命中日志 启用

记录会话日志 启用

会话老化时间 <1-65535>秒

自定义长连接 启用

168 *≤0-24000>小时

确定 取消

步骤 3 提交配置。

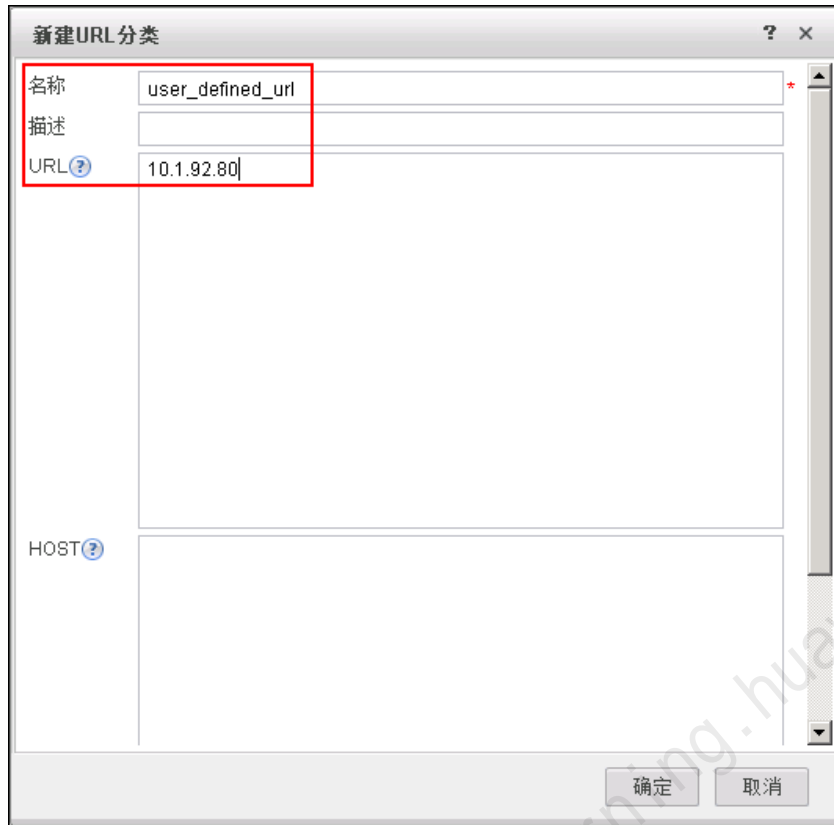
步骤 4 验证结果。

- 内网用户 PC1 无法上传大小超过 2M 的文件到外网的 FTP 服务器；
- 内网用户 PC1 无法从外网 FTP 服务器上下载大小超过 2M 的文件；

1.2.6 任务五：URL 过滤

步骤 1 URL 过滤配置文件。

- 1) 选择“对象 > URL 分类”，新建一条自定义 URL 分类。单击确定完成配置。



- 2) 选择“对象 > 安全配置文件 > URL 过滤”。新建一条 URL 过滤配置文件。在 URL 过滤级别一栏选择自定义，将前一步骤中创建的 URL 分类设置为阻断，并按如图所示将社交网站等设置为阻断。

修改URL过滤配置文件

名称: Profile_URL_1

描述:

动作模式: 严格 松散

缺省动作: 允许

恶意URL检测: 启用

类型	白名单	黑名单
URL	白名单的优先级高于黑名单	白名单的优先级高于黑名单
HOST	白名单的优先级高于黑名单	白名单的优先级高于黑名单

URL过滤级别

高 对所有成人网站，非法活动，社交网络，视频共享等网站进行严格的限制。

中 对所有成人网站和非法网站进行控制。

低 对色情网站进行控制。

自定义

名称	允许	告警	阻断	重标记报文优先级
自定义分类	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	NONE
P2P	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	NONE
下载	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	NONE
人文	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	NONE
体育/运动	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	NONE
社会焦点	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	NONE
军事	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	NONE
社交网络	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	NONE
博彩	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	NONE
休闲	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	NONE
宗教/超自然	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	NONE
性题材	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	NONE
房产/家居	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	NONE
求职招聘	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	NONE

步骤 2 安全策略引用内容安全配置文件。

- 1) 选择“策略>安全策略”，单击新建安全策略“to_Internet”，用于允许内网用户访问外网，并引用内容安全配置文件。



新建安全策略

提示：新建时可以基于策略模板来快速定义您需要的策略。[选择策略模板]

名称 to_internet *

描述

策略组 -- NONE --

源安全区域 trust 修改

目的安全区域 isp1 修改

源地址/地区 请选择或输入地址

目的地址/地区 请选择或输入地址

用户 请选择或输入用户 修改

接入方式 请选择接入方式

终端设备 请选择终端设备

服务 请选择服务

应用 请选择应用或应用组 修改

时间段 any

动作 允许 禁止

内容安全

反病毒 -- NONE -- 配置

入侵防御 -- NONE -- 配置

URL过滤 profile_url_1 配置

文件过滤 -- NONE -- 配置

内容过滤 -- NONE -- 配置

应用行为控制 -- NONE -- 配置

邮件过滤 -- NONE -- 配置

APT防御 -- NONE -- 配置

记录策略命中日志 启用

记录会话日志 启用

会话老化时间 <1-65535>秒

自定义长连接 启用

168 *0-24000>小时

确定 取消

步骤 3 提交配置。

步骤 4 验证结果。

- 在 PC1 上无法访问 <http://10.1.92.80>

1.3 配置参考

```

sysname FW1
#
interface GigabitEthernet1/0/1
undo shutdown
ip address 10.1.50.11 255.255.255.0
#
interface GigabitEthernet1/0/4
undo shutdown
ip address 10.1.71.11 255.255.255.0
#
firewall zone trust
set priority 85
    
```



```
add interface GigabitEthernet1/0/1
#
firewall zone name isp1
  set priority 40
  add interface GigabitEthernet1/0/4
#
firewall interzone trust isp1
  detect ftp
#
profile type app-control name profile_app_1
  http-control file direction upload block-size 102400
  ftp-control file direction upload block-size 102400
  ftp-control file direction download block-size 102400
#
profile type file-block name profile_file_1
  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 Z 7ZIP JAR C CPP JAVA VBS
    application all
    action block
  rule name rule2
    file-type pre-defined name EXE MSI RPM OCX A ELF DLL PE SYS
    application all
    direction download
    action block
profile type file-block name profile_file_2
  rule name rule1
    file-type pre-defined name EXE MSI RPM OCX A ELF DLL PE SYS
    application all
    action block
#
keyword-group name key1
  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 公司违规信息
    expression match-mode text 违规信息
#
profile type data-filter name profile_data_1
  rule name rule
    keyword-group name key1
    file-type all
    application all
    action block
```



```
#
profile type mail-filter name profile_mail_1
  rbl-filter enable
  send-mail anonymity action block
  send-mail attachment max-size 2048 action block
  rcv-mail anonymity action block
  rcv-mail attachment max-size 2048 action block
#
security-policy
  rule name to_Internet
    policy logging
    session logging
    source-zone trust
    destination-zone isp1
    source-address 10.1.11.0 mask 255.255.255.0
    profile app-control profile_app_1
    profile data-filter profile_data_1
    profile file-block profile_file_1
    profile mail-filter profile_mail_1
    action permit
  rule name to_intra_server
    source-zone isp1
    destination-zone trust
    destination-address 10.1.32.0 mask 255.255.255.0
    profile file-block profile_file_2
    profile mail-filter profile_mail_1
    action permit
#
return
```

2 NIP 入侵阻断实验

2.1 实验介绍

2.1.1 关于本实验

入侵防御是一种安全机制。设备通过分析网络流量来检测入侵，并通过一定的响应方式实时地中止入侵行为。本实验介绍如何配置入侵防御功能，保护企业内部用户免受来自 Internet 的攻击。

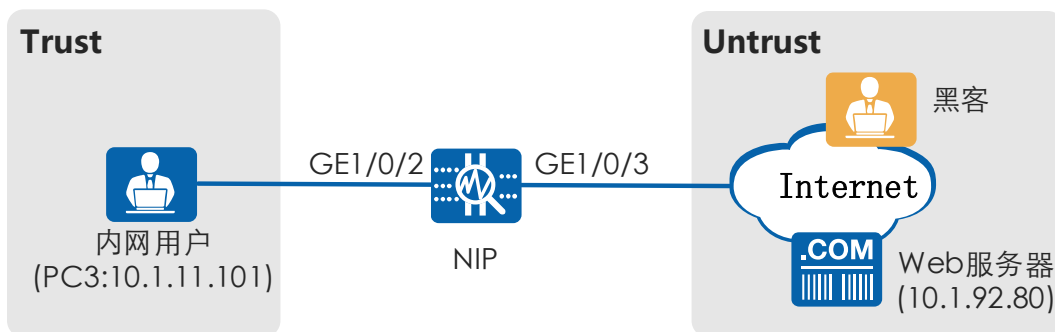
2.1.2 实验目的

内网用户可以访问 Internet。该企业需要在 NIP 上配置入侵防御功能，具体要求如下：

- 企业经常受到蠕虫、木马和僵尸网络的攻击，必须对这些攻击进行防范。
- 避免内网用户访问 Internet 的 Web 服务器时受到攻击。例如，含有恶意代码的网站对内网用户发起攻击。

2.1.3 实验拓扑图

图2-1 安全设备管理实验拓扑图



2.1.4 前提条件

1. 配置防火墙网络连接、IP 地址、接口安全区域。
2. 完成防火墙 FW1 和 FW2 的双机热备组网配置。
3. NAT 策略部署完成。

2.1.5 实验任务列表

序号	任务	任务说明
1	配置入侵防御配置文件	创建入侵防御配置文件，配置签名过滤器。
2	提交入侵防御配置	提交配置。
3	配置安全策略	配置从Trust到Untrust的域间策略。
4	保存配置	查看并导出威胁日志。

2.2 实验任务配置

2.2.1 配置思路

1. 配置安全区域，完成网络基本参数配置。
2. 配置入侵防御配置文件 profile_ips_pc，保护内网用户。通过配置签名过滤器来满足安全需要。
3. 创建安全策略 policy_sec_1，并引用安全配置文件 profile_ips_pc，保护内网用户免受来自 Internet 的攻击。

2.2.2 配置步骤

步骤 1 配置入侵防御配置文件。

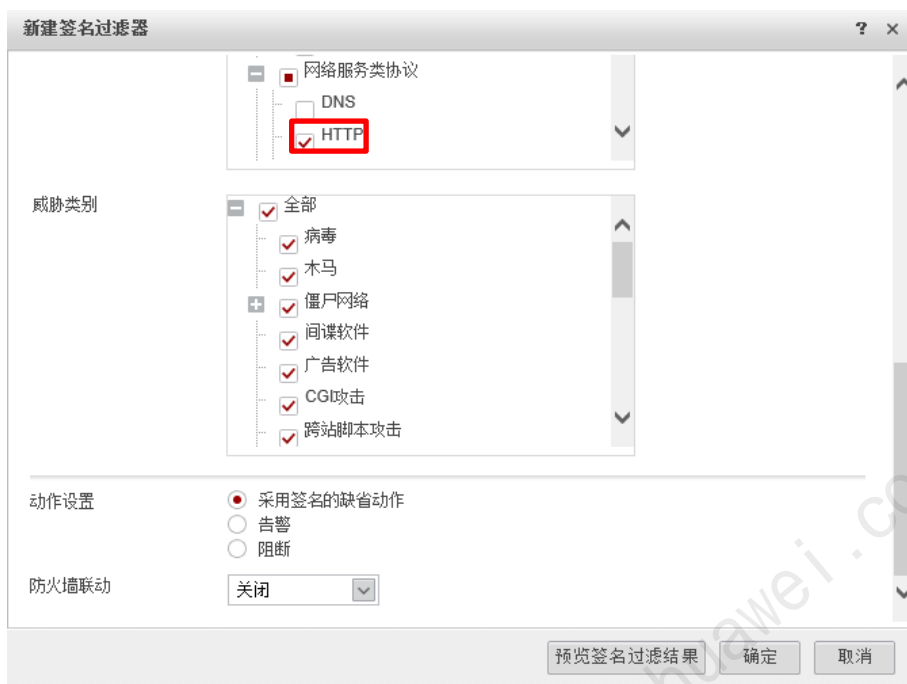
创建入侵防御配置文件 profile_ips，配置签名过滤器。

a. 选择“对象 > 安全配置文件 > 入侵防御”。



b. 配置入侵防御参数。





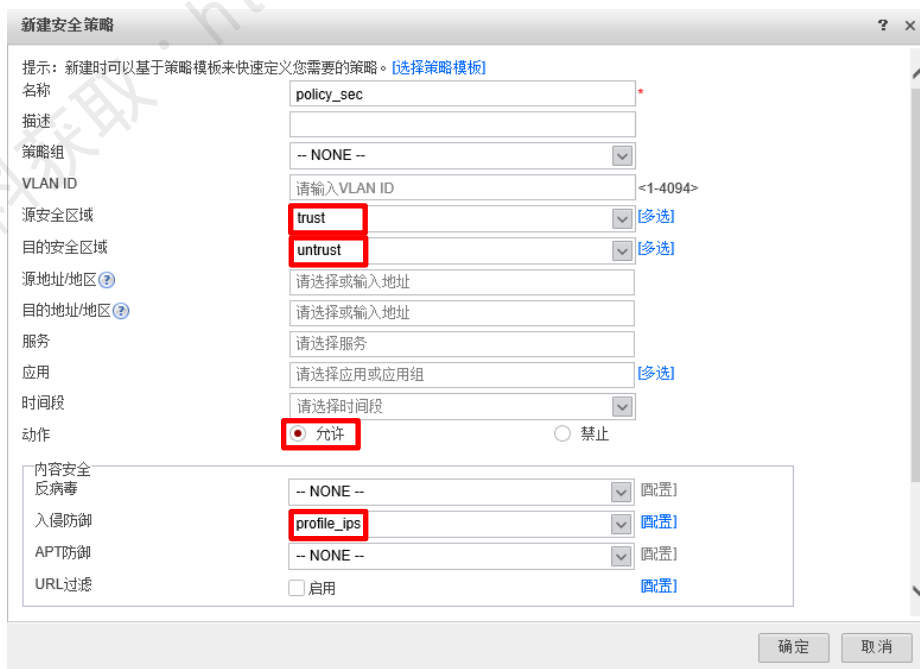
c. 单击“确定”，完成入侵防御配置文件的配置。

步骤 2 提交入侵防御配置。

单击界面右上角的“提交”，在弹出的对话框中单击“确定”。

步骤 3 配置安全策略。

a. 选择“策略 > 安全策略”，单击“新建”，按如下参数配置从 Trust 到 Untrust 的域间策略。



b. 单击“确定”。

步骤 4 保存配置。

单击界面右上角的“保存”，在弹出的对话框中单击“确定”。

步骤 5 结果验证。

在“监控 > 日志 > 业务日志”中，管理员可以定期查看类型为“入侵”的威胁日志信息。

2.3 配置参考

```
#
sysname NIP
#

firewall defend action discard
#
undo dataflow enable
#
sa force-detection enable
#
engine-mode warning
#
firewall dataplane to manageplane application-apperceive default-action drop
#
time-range worktime
period-range 08:00:00 to 18:00:00 working-day
#
interface GigabitEthernet1/0/2
portswitch
undo shutdown
port link-type trunk
port trunk allow-pass vlan 2 to 4094
detect-mode inline
#
interface GigabitEthernet1/0/3
portswitch
undo shutdown
port link-type trunk
port trunk allow-pass vlan 2 to 4094
detect-mode inline
#
firewall zone local
```



```
set priority 100
#
firewall zone trust
set priority 85
add interface GigabitEthernet0/0/0
add interface GigabitEthernet1/0/0
add interface GigabitEthernet1/0/2
add interface GigabitEthernet1/0/4
#
firewall zone untrust
set priority 5
add interface GigabitEthernet1/0/1
add interface GigabitEthernet1/0/3
add interface GigabitEthernet1/0/5
#
firewall zone dmz
set priority 50
#
profile type ips name profile_ips
signature-set name profile_ips
os unix-like windows android ios other
target client
severity high
protocol HTTP
category all
application all
#
profile type url-filter name default
#
sa
#
pair-interface name g1/0/2_to_g1/0/3
pair GigabitEthernet1/0/2 GigabitEthernet1/0/3
#
security-policy
rule name ips_default
disable
profile ips default
action permit
rule name policy_sec
source-zone trust
destination-zone untrust
```



```
profile ips profile_ips  
action permit  
#  
return
```

更多资料获取：<http://learning.huawei.com/cr>

3 应用服务器防病毒攻击实验

3.1 实验介绍

3.1.1 关于本实验

企业内部用户位于 Trust 区域，应用服务器（SMTP 邮件服务器）位于 Trust 区域，Internet 上的用户位于 ISP 1 区域，企业内网用户和 Internet 上的用户使用 SMTP 服务器发邮件。

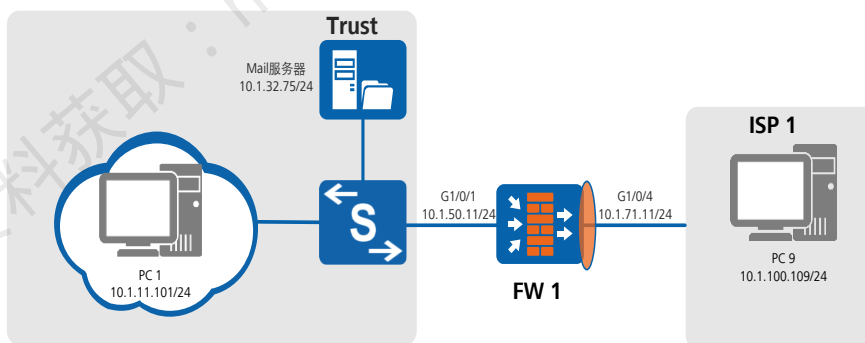
在 FW 上配置 AV 功能，扫描企业内网用户和 Internet 上的用户的 SMTP 邮件中的附件，如果发现用户邮件的附件中带有病毒，则删除附件内容并在邮件正文添加宣告，避免 SMTP 邮件服务器受病毒攻击。

3.1.2 实验目的

- 掌握网关邮件反病毒的工作原理及配置方法；
- 了解 SMTP 的工作原理；

3.1.3 实验拓扑图

应用服务器防病毒攻击实验拓扑图



3.1.4 前提条件

1. 配置防火墙网络连接、IP 地址、接口安全区域。
2. 完成防火墙 FW1 和 FW2 的双机热备组网配置。
3. NAT 策略部署完成。

3.1.5 实验规划

PC 机两台、Mail 服务器一台，交换机一台，USG 系列防火墙 1 台。
按照如下规划配置实验。

表3-1 策略名称规划

名称	备注
安全策略：av_mail	<ul style="list-style-type: none"> • 允许 ISP 1 区域和 Trust 区域的 SMTP 服务和 POP 3 服务互访；
安全策略：mail	<ul style="list-style-type: none"> • 放行 ISP 1 区域和 Trust 区域的 TCP 和 UDP 协议；
安全配置文件：av_mail	<ul style="list-style-type: none"> • ISP 1 区域和 Trust 区域访问 SMTP 服务进行反病毒；
邮件用户名： libai@security.com 密码：Huawei@123	<ul style="list-style-type: none"> • PC 1 上 foxmail 邮箱用户；
邮件用户名： dufu@security.com 密码：Huawei@123	<ul style="list-style-type: none"> • PC 9 上 foxmail 邮箱用户；

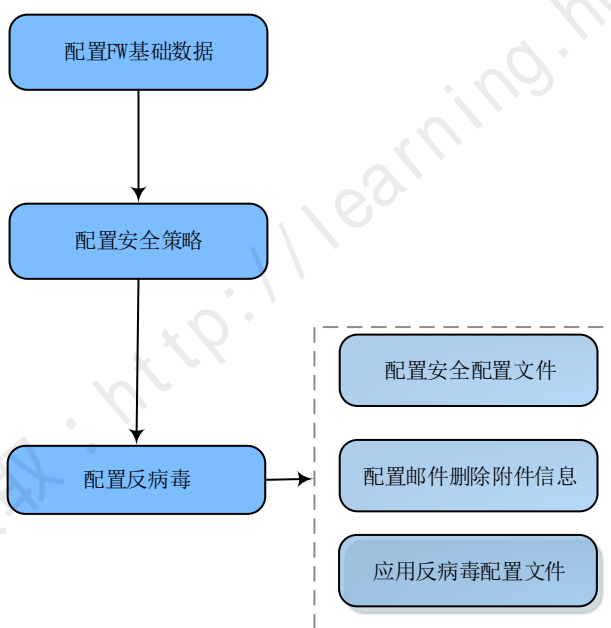
3.1.6 实验任务列表

序号	任务	子任务	备注
1	配置基础数据	安全区域配置	将各接口划分入安全区域；
		安全策略配置	允许ISP 1区域和Trust区域的SMTP服务互访； 放行ISP 1区域和Trust区域的TCP和UDP协议；

2	配置反病毒	配置安全配置文件	ISP 1区域和Trust区域访问SMTP服务进行反病毒配置；
		配置邮件删除附件信息	在邮件正文中添加宣告信息；
		应用反病毒配置文件	在安全策略smtp中应用反病毒配置文件。

3.2 实验任务配置

3.2.1 配置思路

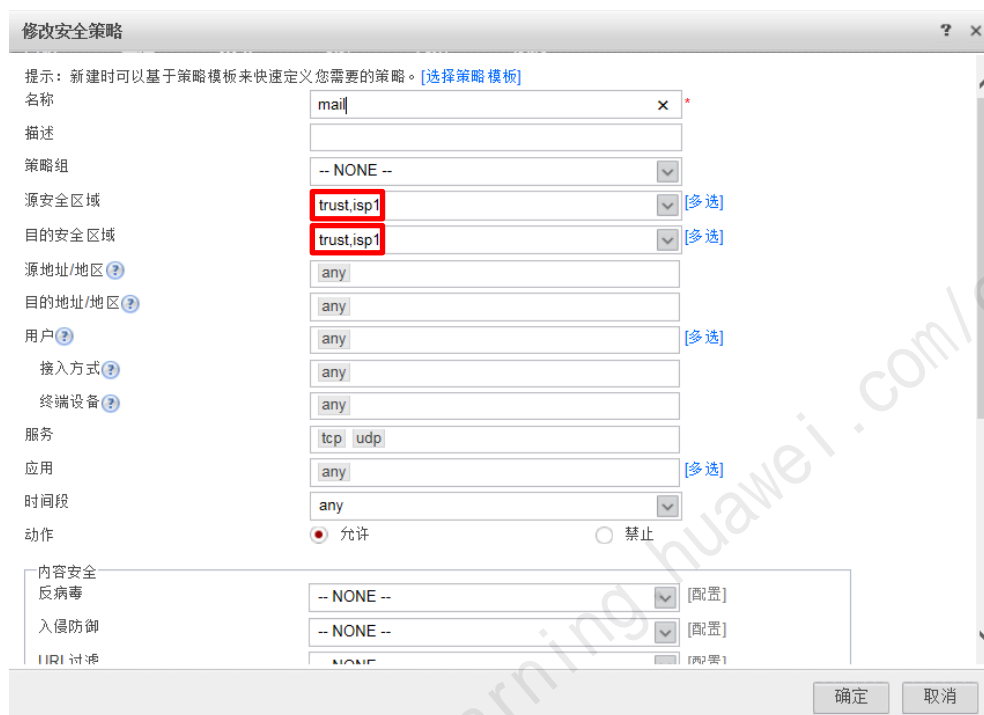


3.2.2 配置步骤

步骤 1 配置 FW1 基本数据。（略）

步骤 2 配置域间防火墙策略。

放行 ISP 1 区域和 Trust 区域的 TCP 和 UDP 协议，邮件的发送基于 TCP，收取基于 UDP。



步骤 3 配置反病毒。

配置反病毒配置文件。选择“对象 >安全配置文件 >反病毒”。在“反病毒配置文件”中单击“+新建”，配置完成后单击“确定”。配置文件完成后单击“提交”。

修改反病毒配置文件

名称: av_mail

描述:

攻击取证: 启用
检测到病毒后, 系统会在设备中获取包含该病毒的数据包。您可以在日志中查看数据包内容。

联动检测: 启用
开启该功能后, 会导致病毒检测的性能降低。安全策略中需要同时引用反病毒和APT防御配置文件, 联动检测功能才会生效。

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 checked="" 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	宣告	告警	告警	告警	阻断

应用例外

请选择应用名称: [v] [添加] [删除]

名称	动作
没有记录	

病毒例外

请输入病毒ID: [] [添加] [删除]

ID	名称
没有记录	

确定 取消

- # 配置邮件删除附件信息。选择“系统 > 配置 > 推送信息配置”。在“邮件删除附件信息”中单击“下载模板”，在下载后的模板中修改推送信息。然后单击“浏览”导入文件。

邮件删除附件信息

名称: 邮件删除附件信息

描述: 删除病毒感染邮件的附件并添加删除信息。

文件格式: TXT

文件大小上限: 1KB

导入文件: [] 浏览... 下载模板

推送信息中必须且只有一个%FILE标识符。

导入 取消

- # 应用反病毒配置文件。选择“策略 > 安全策略 > 安全策略列表”。配置安全策略, 并单击安全策略“mail”的“内容安全”模块选择反病毒配置文件“av_mail”。

修改安全策略

提示: 新建时可以基于策略模板来快速定义您需要的策略。[选择策略模板]

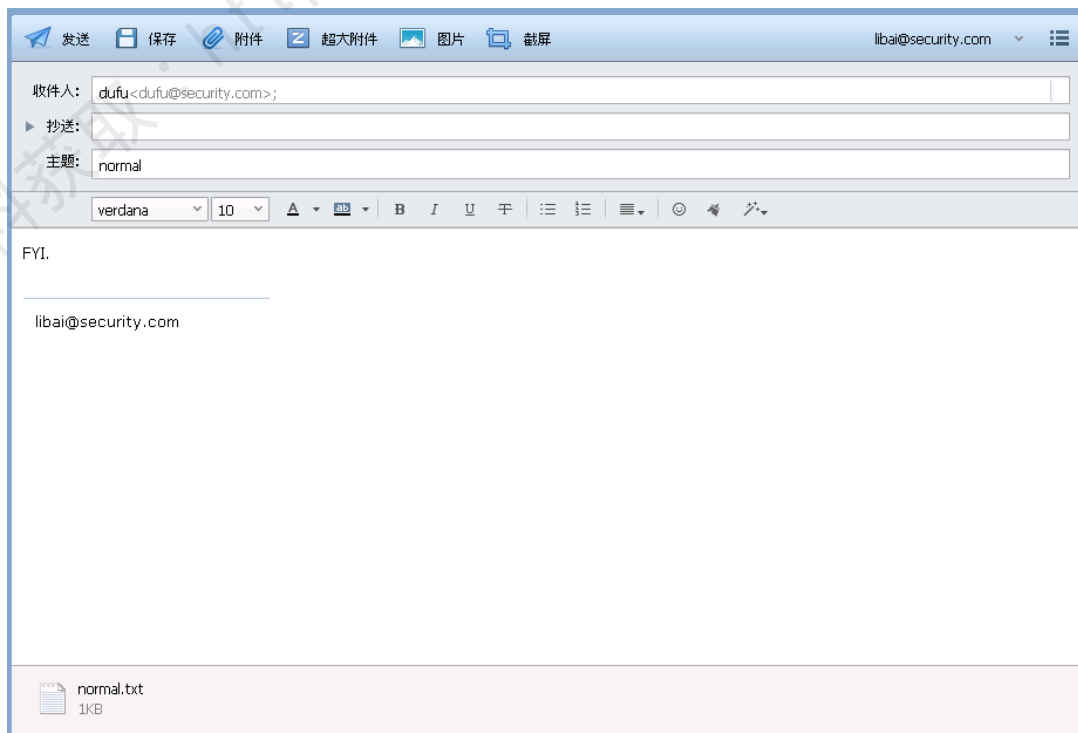
名称	mail
描述	
策略组	-- NONE --
源安全区域	trust.isp1 [多选]
目的安全区域	trust.isp1 [多选]
源地址/地区	any
目的地址/地区	any
用户	any [多选]
接入方式	any
终端设备	any
服务	smtp, pop3
应用	any [多选]
时间段	any
动作	<input checked="" type="radio"/> 允许 <input type="radio"/> 禁止
内容安全	
反病毒	av_mail [配置]
入侵防御	-- NONE -- [配置]
URL 过滤	NONE [配置]

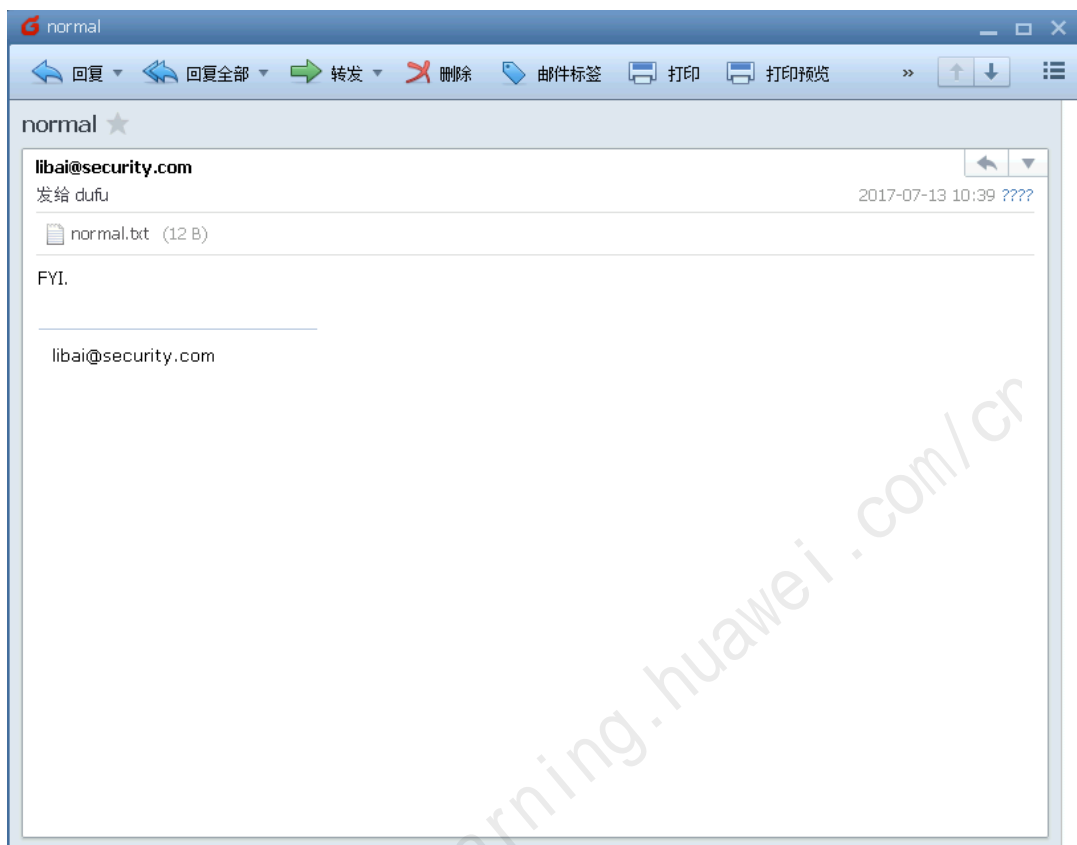
确定 取消

3.3 结果验证

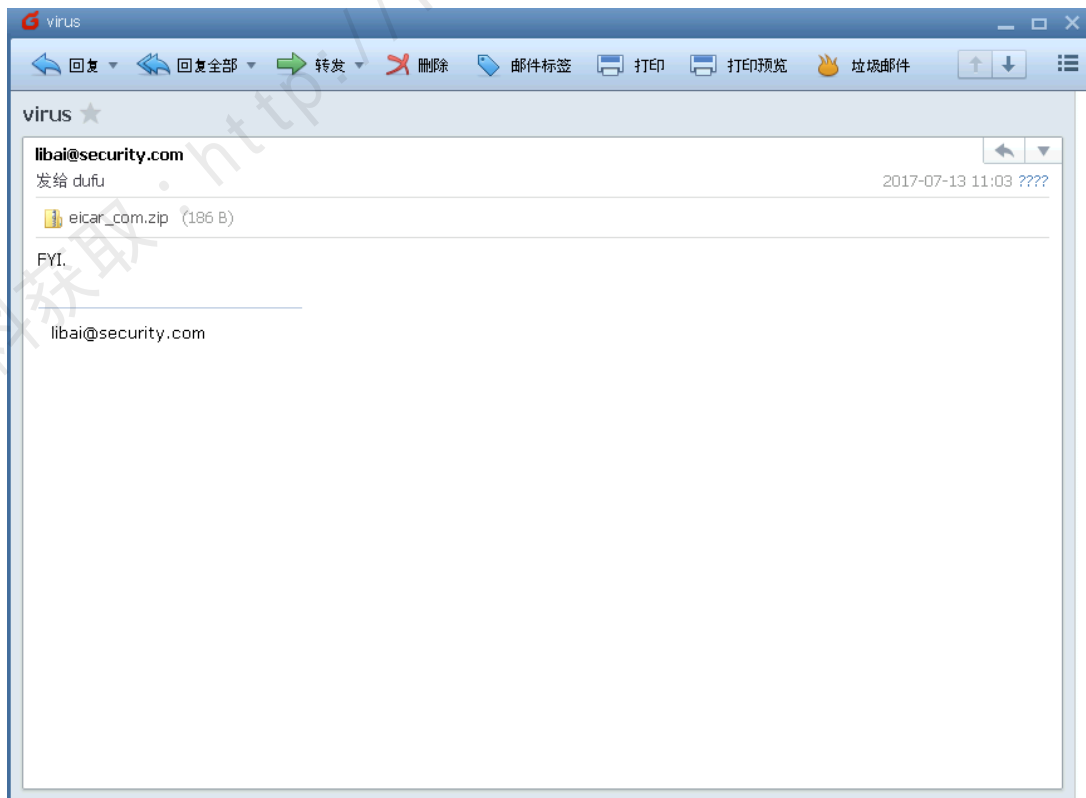
在 PC 1 和 PC 9 上相互用 foxmail 发送附件含有病毒的邮件和正常的邮件，查看结果。

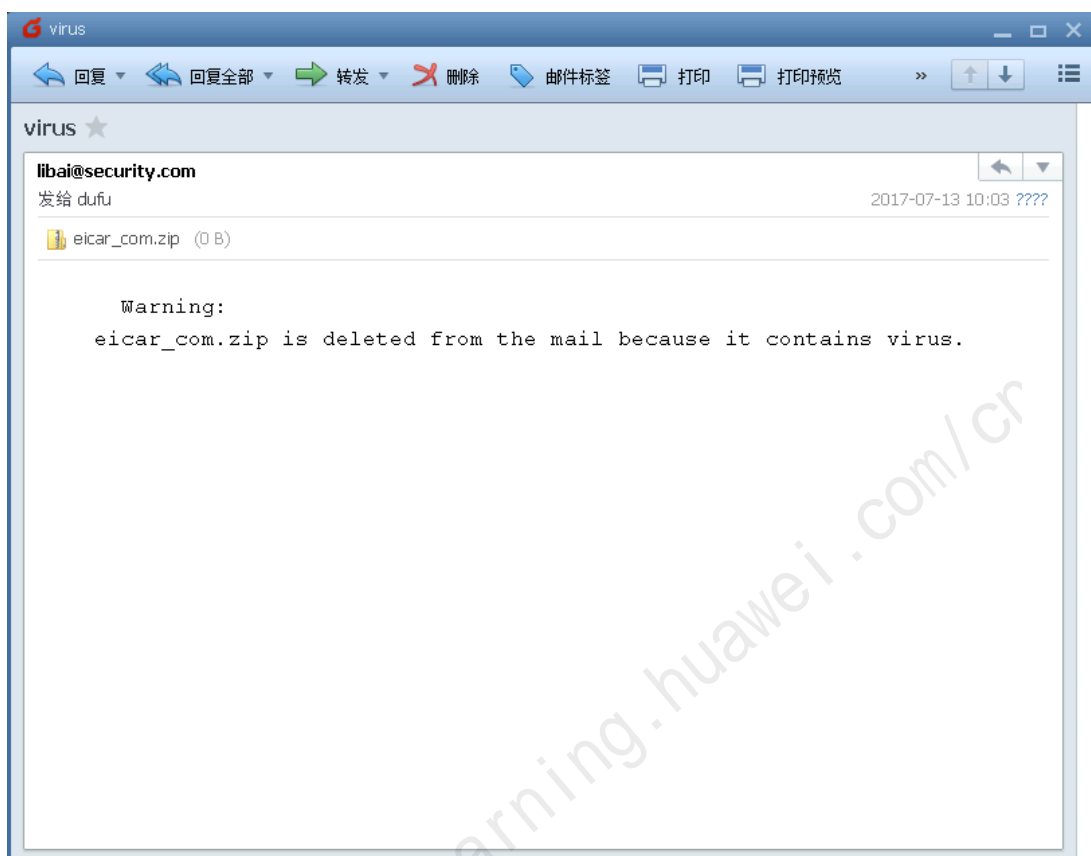
正常收发邮件





发送病毒附件





3.4 配置参考

3.4.1 FW 的配置

```
[FW1]display current-configuration
```

```
#
```

```
sysname FW1
```

```
#
```

```
firewall detect ftp
```

```
#
```

```
firewall zone local
```

```
set priority 100
```

```
#
```

```
firewall zone trust
```

```
set priority 85
```

```
add interface GigabitEthernet1/0/1
```



```
#  
firewall zone name isp1 id 4  
    set priority 40  
    add interface GigabitEthernet1/0/4  
#  
profile type av name av_mail  
    undo http-detect  
    undo ftp-detect  
    smtp-detect action declare  
    undo pop3-detect  
    undo imap-detect  
    undo nfs-detect  
    undo smb-detect  
#  
sa  
#  
security-policy  
    rule name mail  
        source-zone trust  
        source-zone isp1  
        destination-zone trust  
        destination-zone isp1  
        service smtp  
        service pop3  
        profile av av_mail  
        action permit  
#  
return
```

4

内容用户防病毒攻击实验

4.1 实验介绍

4.1.1 关于本实验

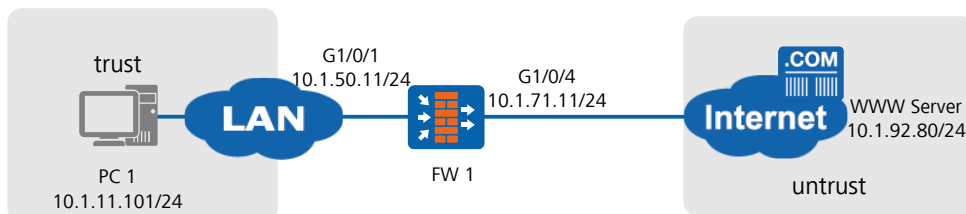
企业内部用户位于 Trust 区域，应用服务器（HTTP 服务器）位于 DMZ 区域，在 FW 上配置 AV 功能，当内网用户访问的网页带病毒时，USG2200 中断访问，并向用户推送一个警告页面提示访问的网页中含病毒。

4.1.2 实验目的

- 掌握内部用户访问 Internet 上的网页时反病毒的工作原理及配置方法；

4.1.3 实验拓扑图

图4-1 内网用户防病毒攻击实验拓扑图



4.1.5 前提条件

1. 配置防火墙网络连接、IP 地址、接口安全区域。
2. 完成防火墙 FW1 和 FW2 的双机热备组网配置。
3. NAT 策略部署完成。

4.1.6 实验规划

PC 机一台、WWW 服务器一台，交换机一台，USG 系列防火墙 1 台。
按照如下规划配置实验。

表4-1 策略名称规划

名称	备注
安全策略: http	<ul style="list-style-type: none"> • 允许 Trust 区域访问 ISP 1 区域的 Http 服务;
地址池: http	<ul style="list-style-type: none"> • PC 1 用于源 NAT 的地址池;
安全配置文件: av_http	<ul style="list-style-type: none"> • Trust 区域访问 ISP 1 区域的 http 阻断病毒;

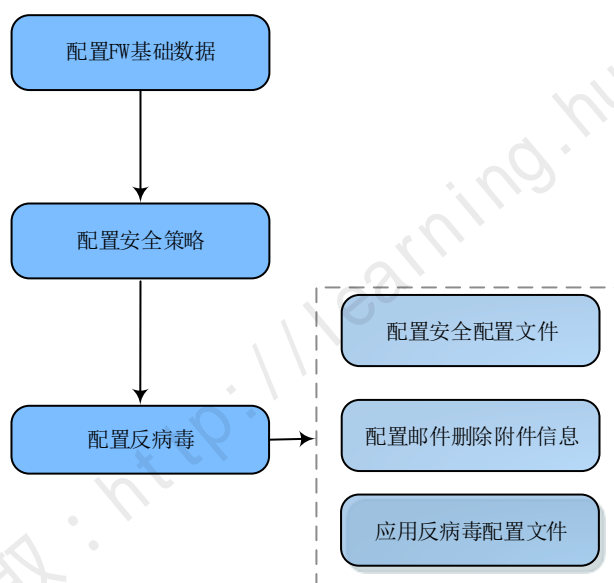
4.1.7 实验任务列表

序号	任务	子任务	备注
1	配置反病毒	配置安全配置文件	对Trust区域访问ISP 1区域的Http服务进行反病毒配置;

		配置病毒文件 阻断信息	配置web阻断推送信息；
		提交反病毒配置	反病毒配置需提交；
2	配置安全策略	安全策略配置	允许Trust区域访问ISP 1区域的Http服务；在安全策略http中应用反病毒配置文件；

4.2 实验任务配置

4.2.1 配置思路



4.2.2 配置步骤

步骤 1 配置反病毒。

配置反病毒配置文件。选择“对象 >安全配置文件 >反病毒”。在“反病毒配置文件中单击“+新建”，配置完成后单击“确定”。配置文件完成后单击“提交”。

修改反病毒配置文件

名称: av_http

描述:

攻击取证: 启用 检测到病毒后, 系统会在设备中获取包含该病毒的数据包。您可以在日志中查看数据包内容。

联动检测: 启用 开启该功能后, 会导致病毒检测的性能降低。安全策略中需要同时引用反病毒和APT防御配置文件, 联动检测功能才会生效。

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 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	

应用例外

病毒例外

确定 取消

配置病毒文件阻断信息。选择“系统 >配置 >推送信息配置”。在“病毒文件阻断配置”中单击“下载模板”，在下载后的模板中修改推送信息。然后单击“浏览”导入文件。

病毒文件阻断配置

名称: 病毒文件阻断配置

描述: 表示访问的WEB页面有病毒, 页面被阻断时推送的页面。

文件格式: TXT、HTML

文件大小上限: 21KB

导入文件: 浏览... **下载模板**

⚠ 请您确保导入文件内容的安全性, 防止推送页面中包含钓鱼网站或木马等恶意信息。

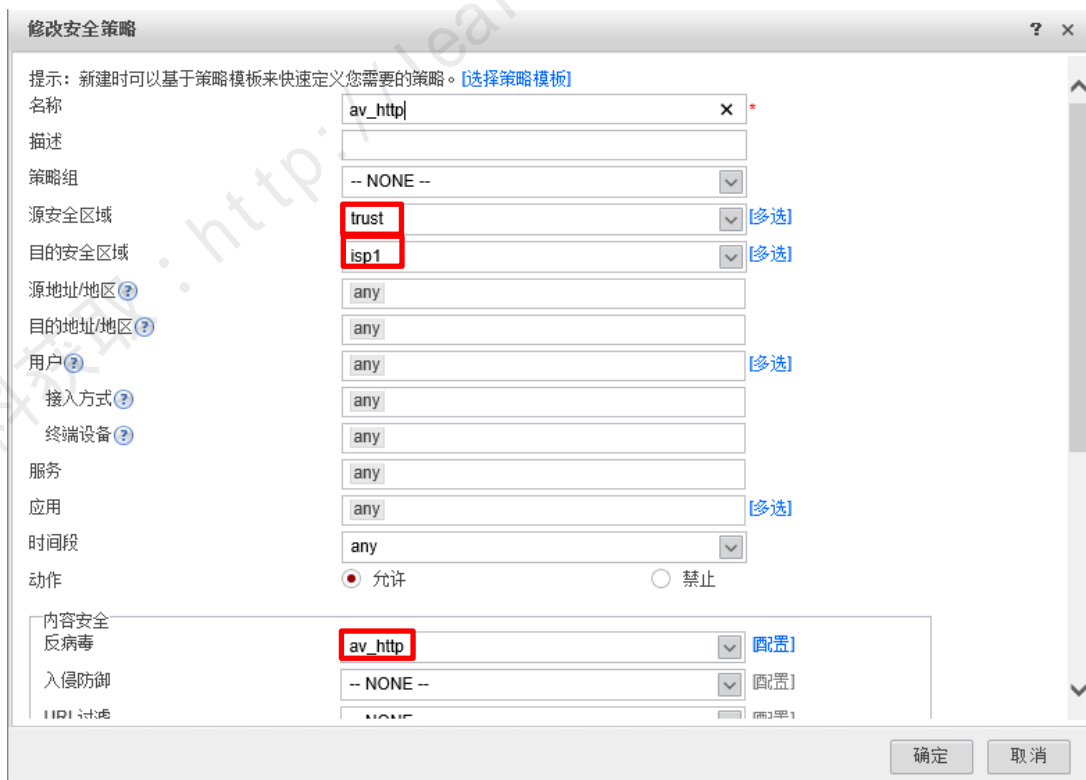
导入 取消

提交反病毒配置。



步骤 2 配置域间防火墙策略。

配置安全策略 http，Trust 域用户可以访问 ISP 区域的 WWW 服务器；应用反病毒配置文件，选择“策略 >安全策略 >安全策略列表”。单击安全策略“http”的“内容安全”模块选择反病毒配置文件“av_http”。



4.3 结果验证

在 PC1 上打开 IE 浏览器，输入“http://10.1.92.80”，查看页面显示。

在 FW1 上选择“监控 > 日志 > 业务日志”，查看防火墙日志。

安全级别	日志类型	时间	日志源	描述
警告	VIRUS	2017/11/1 19:55:13	FW1 WND1AV/4/VIRUS(1) [0]:	AV检测发现病毒。(日志序号=6, 虚拟系统="public", 安全策略="av_http"...

4.4 配置参考

4.4.1 FW 1 的配置

```
<FW1>display current-configuration
#
sysname FW1
#
firewall detect ftp
#
firewall zone local
set priority 100
#
firewall zone trust
set priority 85
add interface GigabitEthernet1/0/1
#
firewall zone name isp1 id 4
set priority 40
add interface GigabitEthernet1/0/4
#
profile type av name av_http
http-detect direction download
undo ftp-detect
undo smtp-detect
undo pop3-detect
```



```
undo imap-detect
undo nfs-detect
undo smb-detect
#
sa
#
security policy
rule name http
source-zone trust
destination-zone isp1
service http
profile av av_http
action permit
#
return
```

更多资料获取：<http://learning.huawei.com/cr>

5

防火墙单包攻击防范实验

5.1 实验介绍

5.1.1 关于本实验

在 DoS 攻击中，单包攻击也是不可小觑的一类威胁，通过在防火墙上启用单包攻击防范功能，可以有效的防止由恶意用户发起的单包攻击。本实验将在防火墙上配置单包攻击防范策略，验证其对此类攻击的防范效果。

5.1.2 实验目的

配置防火墙网络层单包攻击策略，防止外部恶意用户攻击内网资源。

5.1.3 实验拓扑图

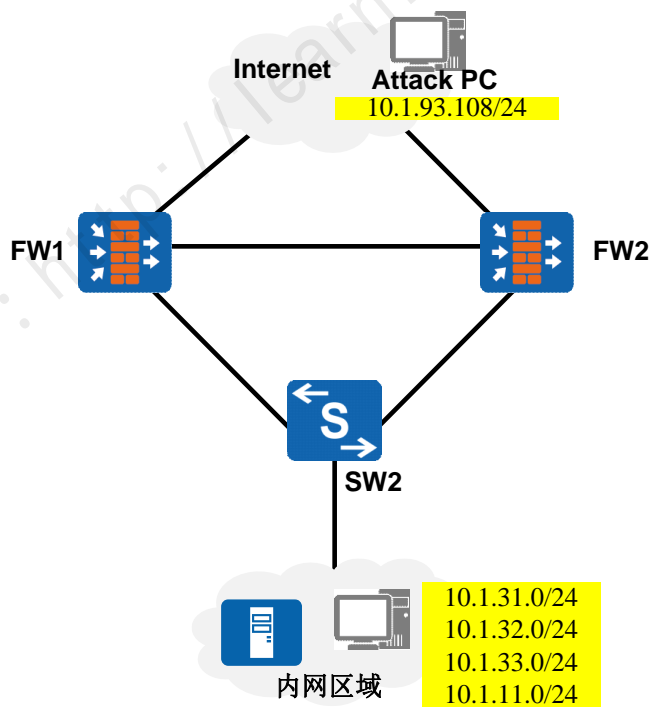


图1-1 1 防火墙单包攻击防范实验拓扑图

5.1.4 前提条件

4. 配置防火墙网络连接、IP 地址、接口安全区域。

5. 完成防火墙 FW1 和 FW2 的双机热备组网配置。
6. NAT 策略部署完成。

5.1.5 实验任务列表

序号	任务	子任务
1	配置防火墙单包攻击防范策略	启用防火墙单包攻击中的防范策略。
	查看日志	在防火墙上查看攻击防范日志，确认防火墙是否阻挡了攻击行为。

5.2 实验任务配置

5.2.1 配置步骤

步骤 1 基本配置。

配置网络连接、IP 地址、接口安全区域及包过滤，放行 isp1/isp2 访问 Trust 区域的流量（具体过程省略）。

步骤 2 配置防火墙单包攻击策略。

选择“策略 > 安全防护 > 攻击防范”，单击“单包攻击”页签，设置“防范动作”为告警。并配置其余防护策略如下图所示：

Anti-DDoS
单包攻击

防范动作 告警 丢弃

配置扫描类攻击防范

地址扫描

最大扫描速率 <1-10000>包/秒

黑名单老化时间 <1-1000>分钟

端口扫描

最大扫描速率 <1-10000>包/秒

黑名单老化时间 <1-1000>分钟

配置畸形报文类攻击防范

IP欺骗攻击防范 IP分片报文检测 Teardrop

Smurf Ping of Death Fraggle

WinNuke Land TCP报文标志合法性检测

配置特殊报文控制类攻击防范

超大ICMP报文控制

最大长度 <28-65535>字节

ICMP不可达报文控制 ICMP重定向报文控制 Tracert

源站选路选项IP报文控制 路由记录选项IP报文控制 时间戳选项IP报文控制

5.3 结果验证

5.3.1 查看防火墙的日志

当防火墙检测到攻击行为后，可通过查看日志了解攻击细节。

(特别提醒：此处已使用模拟软件进行攻击测试。模拟软件仅用于攻防演练及教学测试用途，禁止非法使用。)

选择“监控 > 日志 > 业务日志”，可看到防火墙拦截的攻击行为。

安全级别	日志类型	时间	日志源	描述
警告	FIREWALLATCK	2017/9/20 14:13:28	FW1 %01ATK4/FIR...	攻击类型="Tear drop attack",槽位号="",CPU号="0",接收接口="GE1/0/4",协议="ICMP",攻击源...
警告	FIREWALLATCK	2017/9/20 14:12:58	FW1 %01ATK4/FIR...	攻击类型="Tear drop attack",槽位号="",CPU号="0",接收接口="GE1/0/4",协议="ICMP",攻击源...
警告	FIREWALLATCK	2017/9/20 14:12:28	FW1 %01ATK4/FIR...	攻击类型="IP spoof attack",槽位号="",CPU号="0",接收接口="GE1/0/1",协议="UDP",攻击源地...
警告	FIREWALLATCK	2017/9/20 14:10:28	FW1 %01ATK4/FIR...	攻击类型="IP spoof attack",槽位号="",CPU号="0",接收接口="GE1/0/1",协议="UDP",攻击源地...
警告	FIREWALLATCK	2017/9/20 14:09:58	FW1 %01ATK4/FIR...	攻击类型="IP spoof attack",槽位号="",CPU号="0",接收接口="GE1/0/1",协议="UDP",攻击源地...
警告	FIREWALLATCK	2017/9/20 14:07:58	FW1 %01ATK4/FIR...	攻击类型="IP spoof attack",槽位号="",CPU号="0",接收接口="GE1/0/1",协议="UDP",攻击源地...
警告	FIREWALLATCK	2017/9/20 14:07:28	FW1 %01ATK4/FIR...	攻击类型="IP spoof attack",槽位号="",CPU号="0",接收接口="GE1/0/1",协议="UDP",攻击源地...
警告	FIREWALLATCK	2017/9/20 14:02:58	FW1 %01ATK4/FIR...	攻击类型="IP spoof attack",槽位号="",CPU号="0",接收接口="GE1/0/1",协议="UDP",攻击源地...
警告	FIREWALLATCK	2017/9/20 14:02:28	FW1 %01ATK4/FIR...	攻击类型="IP spoof attack",槽位号="",CPU号="0",接收接口="GE1/0/1",协议="UDP",攻击源地...
警告	FIREWALLATCK	2017/9/20 14:01:58	FW1 %01ATK4/FIR...	攻击类型="IP spoof attack",槽位号="",CPU号="0",接收接口="GE1/0/1",协议="UDP",攻击源地...
警告	FIREWALLATCK	2017/9/20 13:59:27	FW1 %01ATK4/FIR...	攻击类型="IP spoof attack",槽位号="",CPU号="0",接收接口="GE1/0/1",协议="TCP",攻击源地...



5.4 配置参考

5.4.1 FW1 的配置

```
#  
firewall defend port-scan enable  
firewall defend ip-sweep enable  
firewall defend teardrop enable  
firewall defend ip-fragment enable  
firewall defend winnuke enable  
firewall defend fraggle enable  
firewall defend icmp-redirect enable  
firewall defend large-icmp enable  
firewall defend ping-of-death enable  
firewall defend smurf enable  
firewall defend land enable  
firewall defend ip-spoofing enable  
firewall defend action discard  
#
```

更多资料获取：<http://learning.huawei.com/cr>

6

防火墙流量型攻击防范实验

6.1 实验介绍

6.1.1 关于本实验

流量型攻击是 DDoS 攻击中最主要的攻击类型。通过在防火墙上启用 Anti-DDoS 功能，可以有效的防止由恶意用户发起的流量型攻击。本实验将在防火墙上配置 DDoS 攻击防范策略，验证其对此类攻击的防范效果。

6.1.2 实验目的

配置防火墙 SYN Flood 攻击防范策略，防止外部恶意用户攻击内网资源。

6.1.3 实验拓扑图

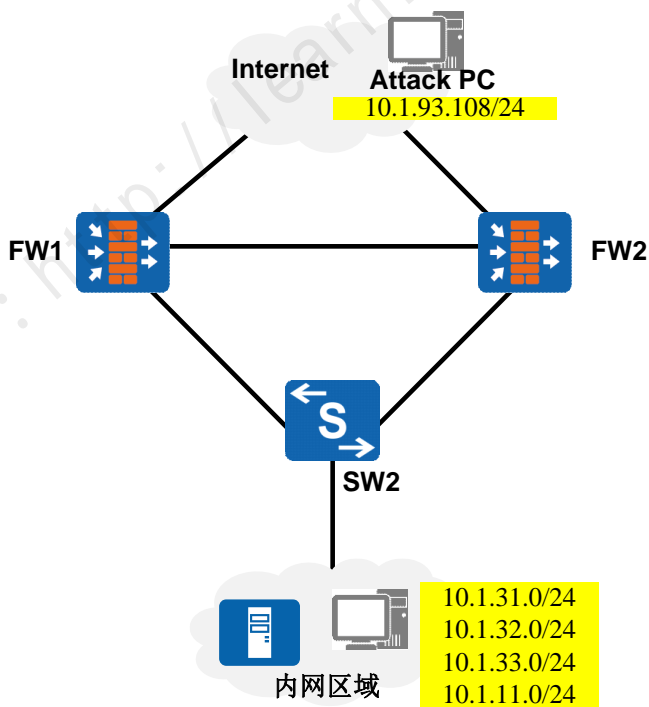


图 2-1 防火墙流量型攻击防范实验拓扑图

6.1.4 前提条件

1. 配置防火墙网络连接、IP 地址、接口安全区域。

2. 完成防火墙 FW1 和 FW2 的双机热备组网配置。
3. NAT 策略部署完成。

6.1.5 实验任务列表

序号	任务	子任务
1	配置防火墙Anti-DDoS防范策略	配置SYN Flood防范策略。
	查看日志	在防火墙上查看攻击防范日志, 确认防火墙是否阻挡了攻击行为。

6.2 实验任务配置

6.2.1 配置步骤

步骤 1 基本配置

配置网络连接、IP 地址、接口安全区域及包过滤（具体过程省略）。

步骤 2 配置防火墙 Anti-DDoS 防御模式及接口。

1. 选择“策略 > 安全防护 > 攻击防范”，在 Anti-DDoS 页签下，配置“防御模式”为检测，选择 G1/0/4 及 G1/0/5 接口为检测接口。



2. 在 DDoS 栏，点击“配置学习参数”，启用流量学习功能。学习周期为每天，每次学习 1 小时。配置完成后，点击“确定”。

配置学习参数 ? x

启用“学习功能”后，系统将自动分析当前流量并计算出各种攻击类型的建议防范阈值。计算结果将显示在“DDoS”界面的“学习结果”列中。您可以参考该结果手工设定阈值，或者在本界面中勾选“自动应用”的“启用”，将学习结果自动应用到阈值中。

学习功能 启用

每次学习时长 <1-24>

学习模式 单次学习 周期学习

周期学习间隔 <1-365>

自动应用 启用

学习容忍度 <0-4000>

3. 选择启用 SYN Flood 攻击防范技术。保持默认阈值。配置完成后点击“应用”。

DDoS

配置学习参数 应用学习结果

学习状态：正在学习

攻击类型	防范技术	启用	阈值
SYN Flood	源探测	<input checked="" type="checkbox"/>	2000 <1-8000000>pps
	指纹防范	<input type="checkbox"/>	50 <1-10240>Mbps
UDP Flood	分片指纹防范	<input type="checkbox"/>	50 <1-10240>Mbps
	限流	<input type="checkbox"/>	50 <1-10240>Mbps
ICMP Flood	限流	<input type="checkbox"/>	2000 <1-1200000>pps
HTTP Flood	<input checked="" type="radio"/> 基础源探测 <input type="radio"/> 302重定向 <input type="radio"/> 高级源探测	<input type="checkbox"/>	8000 <1-80000000>pps
HTTPS Flood	源探测	<input type="checkbox"/>	2000 <1-80000000>pps
DNS Request Flood	<input checked="" type="radio"/> 源探测 <input type="radio"/> CNAME重定向	<input type="checkbox"/>	2000 <1-80000000>pps
DNS Response Flood	源探测	<input type="checkbox"/>	2000 <1-80000000>pps
SIP Flood	源探测	<input type="checkbox"/>	2000 <1-80000000>pps

6.3 结果验证

6.3.1 查看防火墙的日志

当防火墙检测到攻击行为后，可通过查看日志了解攻击细节。

特别提醒：此处已使用模拟软件进行攻击测试。模拟软件仅用于攻防演练及教学测试用途，禁止非法使用。

选择“监控 > 日志 > 业务日志”，可查看到防火墙拦截的攻击行为。

业务日志列表

导出 刷新 请选择安全级别

安全级别	日志类型	时间	日志源	描述
警告	FIREWALLATCK	2017/9/20 15:14:58	FW1 %%01ATK4/FIREWALLATCK(0)[0]	攻击类型="IP spoof attack", 槽位号="", CPU号="0", 接收接口="GE1/0/1", 协议
警告	FIREWALLATCK	2017/9/20 15:14:58	FW1 %%01ATK4/FIREWALLATCK(0)[1]	攻击类型="Syn flood attack", 槽位号="", CPU号="0", 接收接口="GE1/0/4", 协
警告	FIREWALLATCK	2017/9/20 15:14:28	FW1 %%01ATK4/FIREWALLATCK(0)[2]	攻击类型="IP spoof", 攻击类型="Syn flood attack", 槽位号="", CPU号="0", 接收接口="GE1/0/4", 协议="TCP", 攻击源地
警告	FIREWALLATCK	2017/9/20 15:13:58	FW1 %%01ATK4/FIREWALLATCK(0)[3]	攻击类型="IP spoof", 地址="10.1.93.193:10096 10.1.93.195:10098 10.1.93.196:10099 10.1.93.197:10100 10.1.93.198:10000 10.1.93.199:10001 10.1.93.200:10002 10.1.93.201:10003 10.1.93.203:10005 10.1.93.204:10006 10.1.93.202:10004", 攻击目的地址="10.1.71.11", 攻击开始时间="2017-9-20 15:14:35", 攻击结束时间="2017-9-20 15:14:57", 攻击报文个数="1528993", 攻击速率="73614", 用户="", 动作="discard".
警告	FIREWALLATCK	2017/9/20 15:12:58	FW1 %%01ATK4/FIREWALLATCK(0)[4]	攻击类型="IP spoof
警告	FIREWALLATCK	2017/9/20 15:07:58	FW1 %%01ATK4/FIREWALLATCK(0)[5]	攻击类型="IP spoof
警告	FIREWALLATCK	2017/9/20 15:04:58	FW1 %%01ATK4/FIREWALLATCK(0)[6]	攻击类型="IP spoof
警告	FIREWALLATCK	2017/9/20 15:04:28	FW1 %%01ATK4/FIREWALLATCK(0)[7]	攻击类型="IP spoof
警告	FIREWALLATCK	2017/9/20 15:03:58	FW1 %%01ATK4/FIREWALLATCK(0)[8]	攻击类型="IP spoof attack", 槽位号="", CPU号="0", 接收接口="GE1/0/1", 协议
警告	FIREWALLATCK	2017/9/20 15:02:58	FW1 %%01ATK4/FIREWALLATCK(0)[9]	攻击类型="IP spoof attack", 槽位号="", CPU号="0", 接收接口="GE1/0/1", 协议

6.4 配置参考

6.4.1 FW1 的配置

```
#
interface GigabitEthernet1/0/4
anti-ddos flow-statistic enable
#
interface GigabitEthernet1/0/5
anti-ddos flow-statistic enable
#
anti-ddos syn-flood source-detect
anti-ddos baseline-learn start
anti-ddos baseline-learn mode loop
anti-ddos baseline-learn learn-duration 60
anti-ddos baseline-learn learn-interval 1440
#
```