

## FortiGate Email DLP

版本	1.0
时间	2012 年 1 月
作者	胡丹丹(ddhu@fortinet.com)
支持的版本	FOS v4.X
状态	草稿

## 目录

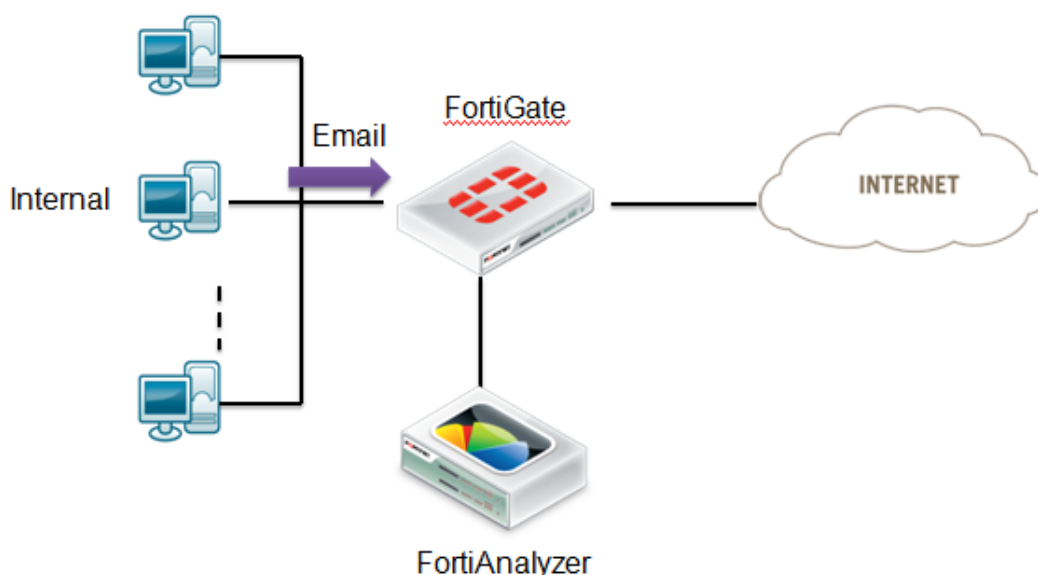
1. 目的 .....	3
2. 环境介绍 .....	3
3. DLP 介绍 .....	4
3.1 DLP 传感器 .....	4
3.2 DLP 规则 .....	5
3.3 混合规则 .....	6
4. Email DLP 设定 .....	6
4.1 FortiGate DLP 设定 .....	7
4.2 DLP 传感器定义 .....	7
4.3 策略调用 DLP .....	8
4.4 定义 FortiAnalyzer .....	9
5. 查看归档 .....	10
6. 参考 .....	10

## 1. 目的

FortiGate DLP(Data leak prevention)数据泄露保护可以阻止内部敏感数据信息泄露,当在 DLP 设置中定义敏感数据的字符,被匹配的数据流经 FortiGate 时将被阻断,记录或允许。也可以通过基于文件类型,文件大小,正则表达式及高级规则及复合规则定义 DLP 传感器实现安全策略。DLP 功能不仅能阻止内部敏感数据向外部泄露,也同样能阻止非法信息流入内部网络。本文就 FortiGate 的 Email DLP 功能进行说明。

## 2. 环境介绍

本文使用 1 台 FortiGate-1240B 及 FortiAnalyzer 2000B 进行说明,本文使用的系统版本为 FortiOS v4.0MR2 Patch8,FAZ v4.00MR2 Patch5。



## 3. DLP 介绍

### 3.1 DLP 传感器

DLP 传感器是一系列 DLP 规则的合集,通过策略中调用该传感器,对数据中匹配的字符根据预定义的动作允许、阻止、记录相关数据。DLP 过滤器中包含各种过滤条件,如文件类型,文件大小,通过正则表达式定义敏感字符等等。

FortiGate 系统默认自带若干已定义 DLP 传感器。



每个传感器可以由若干规则或组合规则组合而成。



针对设定规则,设定相关动作以及是否进行存档等等。

动作 无

存档 无

严格 屏蔽

成员类型 例外

封禁

封禁发送者

隔离源IP地址

隔离源接口

All-Email

## 3.2 DLP 规则

DLP 过滤规则支持以下协议 Email,HTTP,FTP,NNTP,IM 及如下各个不同协议下过滤字段的数据定义。

新建/编辑普通规则

名字 All-HTTP

声明

协议 HTTP

规则

发送  HTTP 接收  HTTP 发送  HTTP 接收

规则

- 总是
- 主体
- URL
- 传输大小   KB
- Cookie
- CGI参数
- HTTP头部
- 主机名
- 文件类型  存在于
- 二进制文件格式 (BASE64)
- 认证用户
- 用户组
- 文件  加密的

## 3.3 混合规则

混合规则有一个或若干普通规则组合而成,定义混合规则之前需要定义普通规则后加入混合规则。

新建/编辑混合规则

名字

注释

协议

SMTP  IMAP  POP3  SMTPS  IMAPS  POP3S

规则

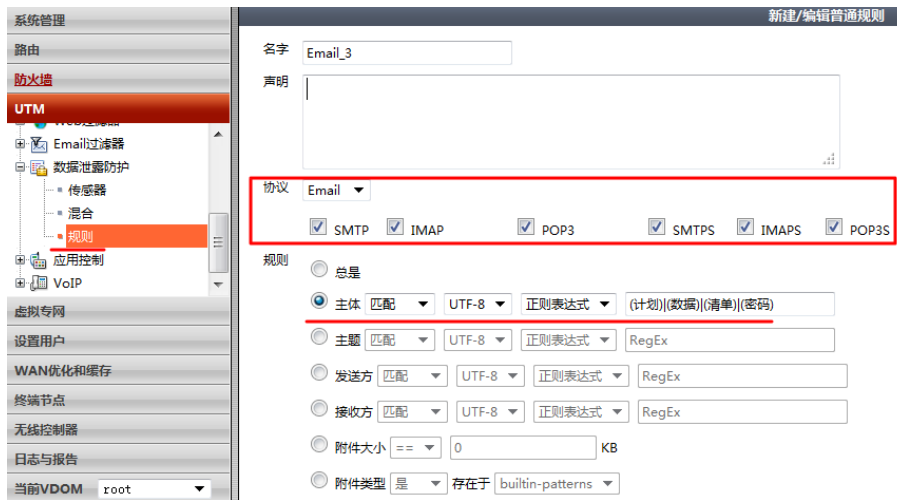
OK 取消

## 4. Email DLP 设定

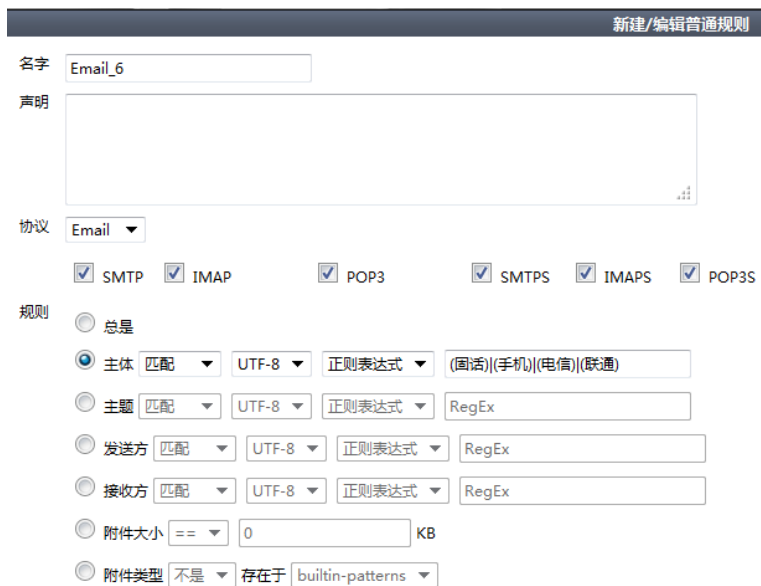
本文就 Email DLP 邮件归档设定进行举例,其他诸如 HTTP,FTP 等定义请参考 Email DLP 设定。全部标题及内容归档需要 FortiAnalyzer 方可实现该需求。

## 4.1 FortiGate DLP 设定

UTM-规则-定义数据泄露保护规则,此处以邮件主体使用 UTF-8 编码,启用正则表达式中匹配“(计划)|(数据)|(清单)|(密码)”中任意词汇,作为过滤条件。



定义多个 dlp 条件,则继续添加 dlp 规则。

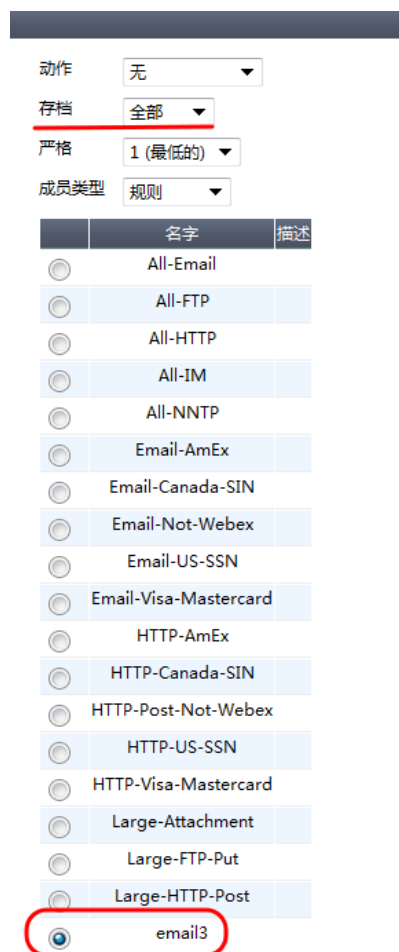


## 4.2 DLP 传感器定义

新建 DLP 传感器,创建新规则,将之前定义的规则。



此例仅对 Email 主体含有关键字内容进行归档,不作其他动作。



## 4.3 策略调用 DLP

在相应的策略中启用协议选项,如无特殊需求,使用 default 即可,再启用 DLP



传感器调用之前定义的 DLP 传感器。

**编辑**

源接口/区	port37(FG1240B--to--neiwang)
源地址	all <span style="float: right;">多个</span>
目的接口/区	port38(FG1240B--to--6509)
目的地址	all <span style="float: right;">多个</span>
时间表	always
服务	ANY <span style="float: right;">多个</span>
动作	ACCEPT

记录允许流量

---

**NAT**

不使用 NAT  
 启用 NAT  动态IP地址池  
 使用中央NAT表

---

启用基于用户认证的策略

---

**UTM**

<input checked="" type="checkbox"/> 协议选项	default
<input type="checkbox"/> 启用病毒检测	[请选择]
<input type="checkbox"/> 启用IPS	[请选择]
<input checked="" type="checkbox"/> 启用Web过滤器	wangyeguolv
<input type="checkbox"/> 启用email过滤器	[请选择]
<input checked="" type="checkbox"/> 启用DLP传感器	xianyang--dlp
<input checked="" type="checkbox"/> 白名单控制	shininwangzhan

## 4.4 定义 FortiAnalyzer

在日志设定中定义日志接收 FortiAnalyzer 地址

系统管理
日志设置

日志与报告

- 日志配置
- 日志设置
- E-mail报警

远程记录&存档

FortiAnalyzer设备设置

IP 地址: 1.1.1.1 测试连接

最低日志级别: 信息

缓存到硬盘并上传 每天 at 00:00 (hh:mm)

当日志硬盘已满: 覆盖最老的日志

开启IPS存档记录

FortiGuard 分析及管理服务 [Settings]

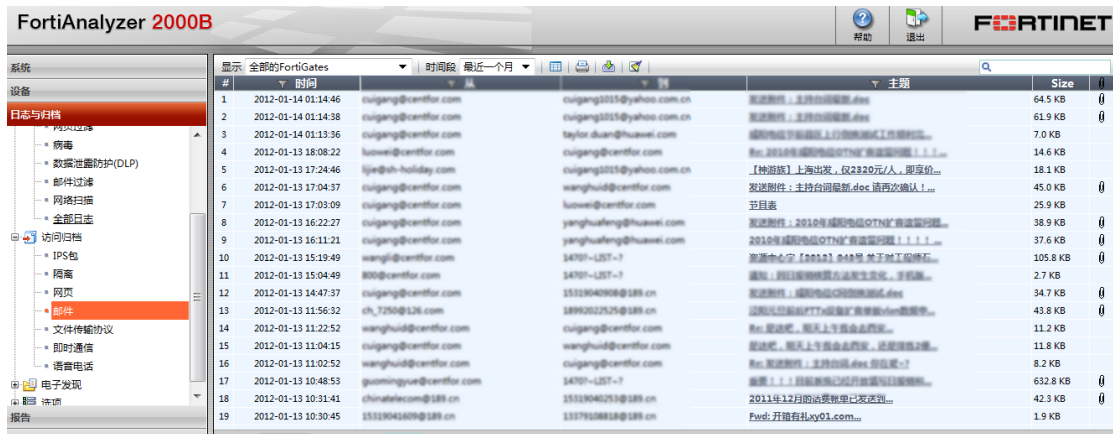
syslog服务器设置

**应用**

## 5. 查看归档

登陆 FortiAnalyzer 可以查看所有匹配 DLP 过滤规则的日志及邮件归档

点击邮件链接可以查看具体邮件内容。



#	时间	从	到	主题	Size
1	2012-01-14 01:14:46	cuiqiang@centfor.com	cuiqiang1015@yahoo.com.cn	发送附件：主舞台背景图.doc	64.5 KB
2	2012-01-14 01:14:38	cuiqiang@centfor.com	cuiqiang1015@yahoo.com.cn	发送附件：主舞台背景图.doc	61.9 KB
3	2012-01-14 01:13:36	cuiqiang@centfor.com	taylor_duan@huawei.com	深圳地区于和路路上行线快线施工期间公告	7.0 KB
4	2012-01-13 18:08:22	luwei@centfor.com	cuiqiang@centfor.com	Re: 2010年福州电信OTN'有谁知道!!!	14.6 KB
5	2012-01-13 17:24:46	ljq@sh-holiday.com	cuiqiang1015@yahoo.com.cn	【特约稿】上海出发，仅2820元/人，更低价...	18.1 KB
6	2012-01-13 17:04:37	cuiqiang@centfor.com	wanghui@centfor.com	发送附件：主舞台背景图.doc 请再次确认！...	45.0 KB
7	2012-01-13 17:03:09	cuiqiang@centfor.com	luwei@centfor.com	目录表	25.9 KB
8	2012-01-13 16:22:27	cuiqiang@centfor.com	yangshufeng@huawei.com	发送附件：2010年福州电信OTN'有谁知道!!!	38.9 KB
9	2012-01-13 16:11:21	cuiqiang@centfor.com	yangshufeng@huawei.com	2010年福州电信OTN'有谁知道!!!	37.6 KB
10	2012-01-13 15:19:49	wanghui@centfor.com	14701-1217-7	客服中心：[2012] 648号 关于下工位修...	105.8 KB
11	2012-01-13 15:04:49	800@centfor.com	14701-1217-7	通知：浙江家网网管方法发生更改，予以通...	2.7 KB
12	2012-01-13 14:47:37	cuiqiang@centfor.com	15119040908@189.cn	发送附件：福州电信OTN'有谁知道!!!	34.7 KB
13	2012-01-13 11:56:32	ch_7250@126.com	18992022525@189.cn	过机儿总机机PTT-设备扩展参数表.xlsx-数据中...	43.8 KB
14	2012-01-13 11:22:52	wanghui@centfor.com	cuiqiang@centfor.com	Re: 发送吧，明天上午我会去西安。	11.2 KB
15	2012-01-13 11:04:15	cuiqiang@centfor.com	wanghui@centfor.com	发送吧，明天上午我会去西安，这是植物之...	11.8 KB
16	2012-01-13 11:02:52	wanghui@centfor.com	cuiqiang@centfor.com	Re: 发送附件：主舞台背景图.doc 各位呢？	8.2 KB
17	2012-01-13 10:48:53	guomingyue@centfor.com	14701-1217-7	请发上!!!目前设备已运行故障予以维修。	632.8 KB
18	2012-01-13 10:31:41	china telecom@189.cn	15119040253@189.cn	2011年12月的话费账单已发送到...	42.3 KB
19	2012-01-13 10:30:45	15119040809@189.cn	13379108818@189.cn	Pwd: 开港有礼ay01.com...	1.9 KB

## 6. 参考

[UTM](#)

[Using FortiGate DLP to block/filter email/spam based on "sender" \(From:\) information](#)