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

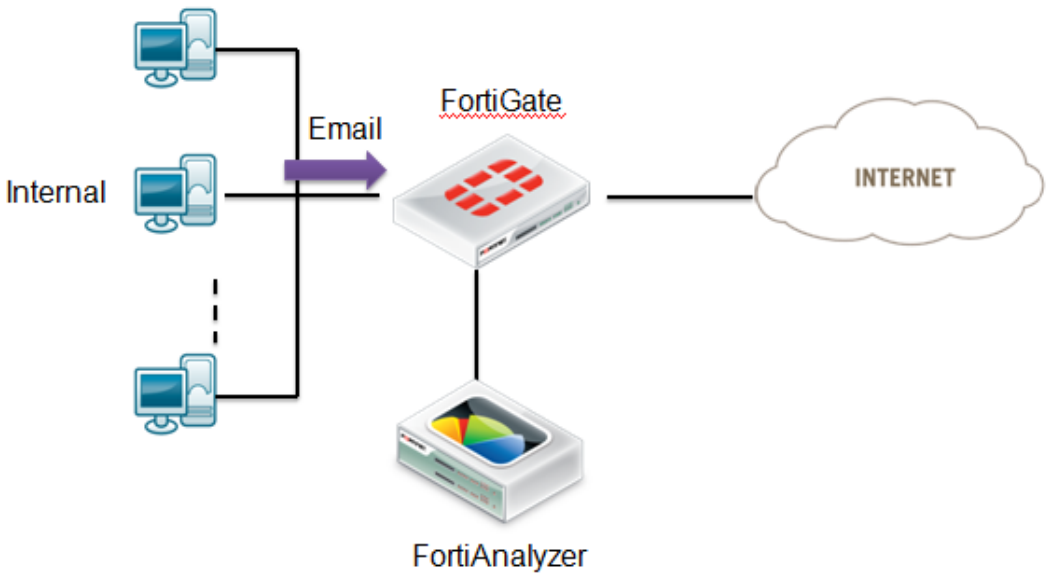
目录

1. 目的

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 ForitGate 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。

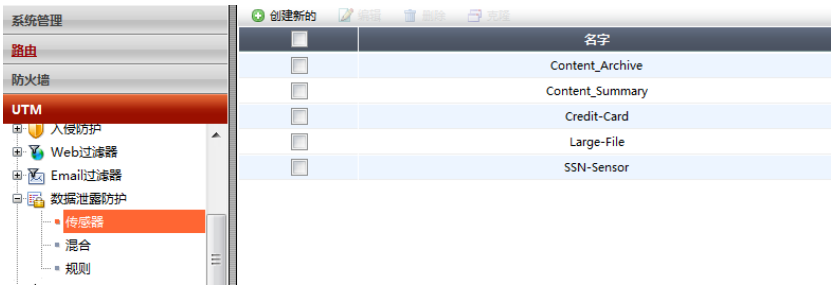


3. DLP 介绍

3.1 DLP 传感器

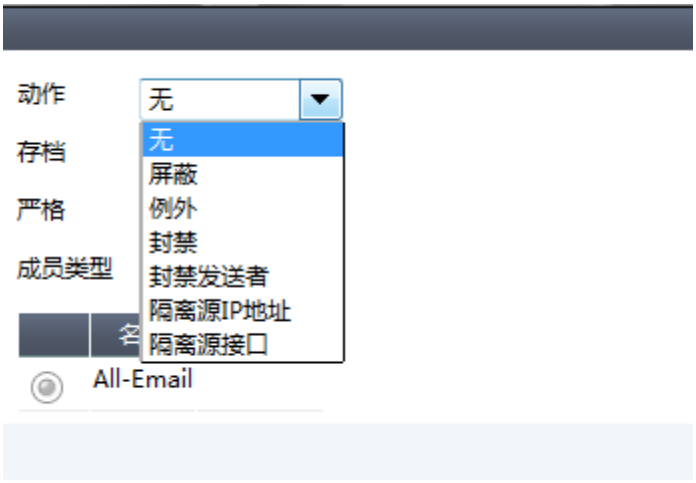
DLP 传感器是一系列 DLP 规则的合集,通过策略中调用该传感器,对数据中匹配的字符根据预定义的动作允许、阻止、记录相关数据。DLP 过滤器中包含各种过滤条件,如文件类型,文件大小,通过正则表达式定义敏感字符等等。

FortiGate 系统默认自带若干已定义 DLP 传感器。



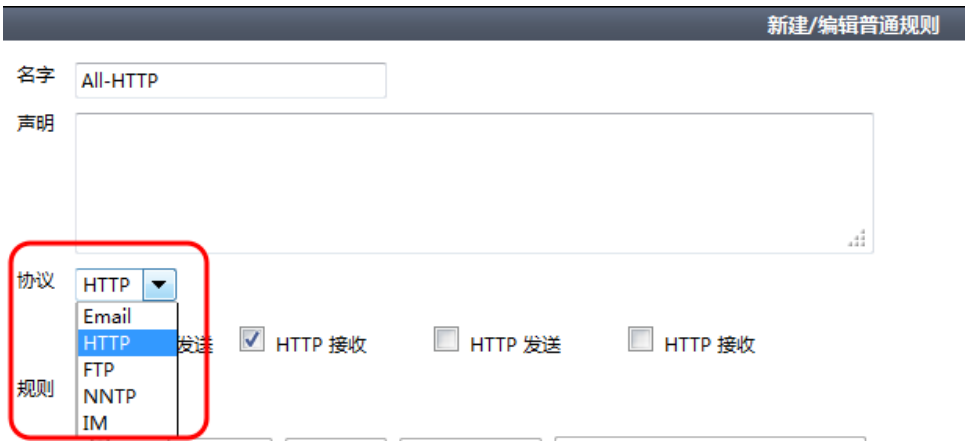
每个传感器可以由若干规则或组合规则组合而成。

针对设定规则,设定相关动作以及是否进行存档等等。



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。



3.3 混合规则

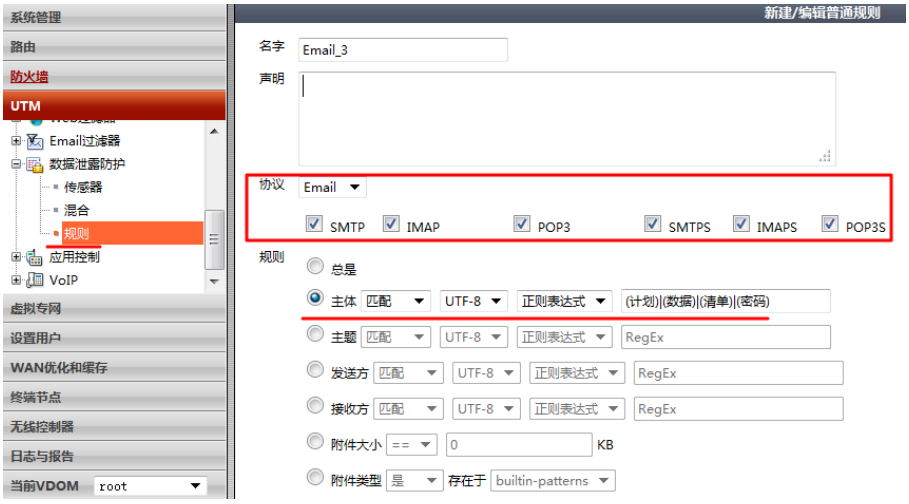
混合规则有一个或若干普通规则组合而成,定义混合规则之前需要定义普通规则后加入混合规则。

4. Email DLP 设定

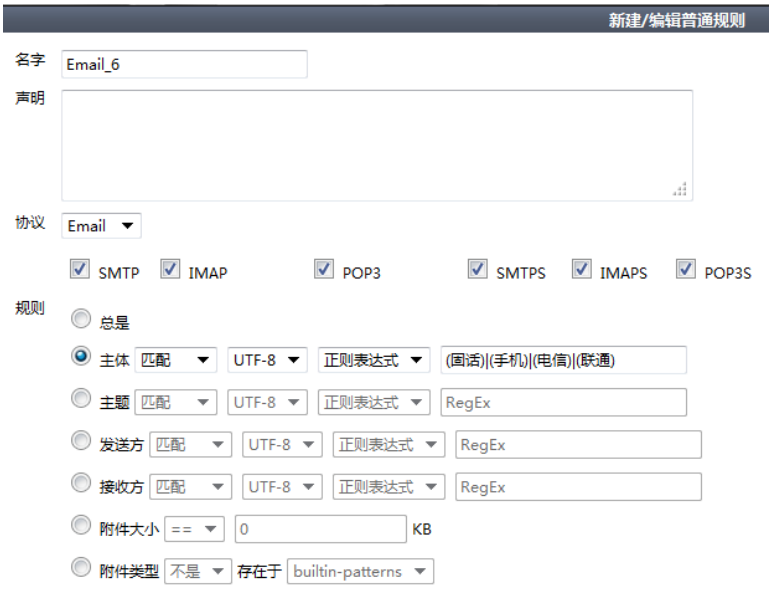
本文就 Email DLP 邮件归档设定进行举例,其他诸如 HTTP,FTP 等定义请参考 Email DLP 设定。全部标题及内容归档需要 FortiAnalyzer 方可实现该需求。

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。



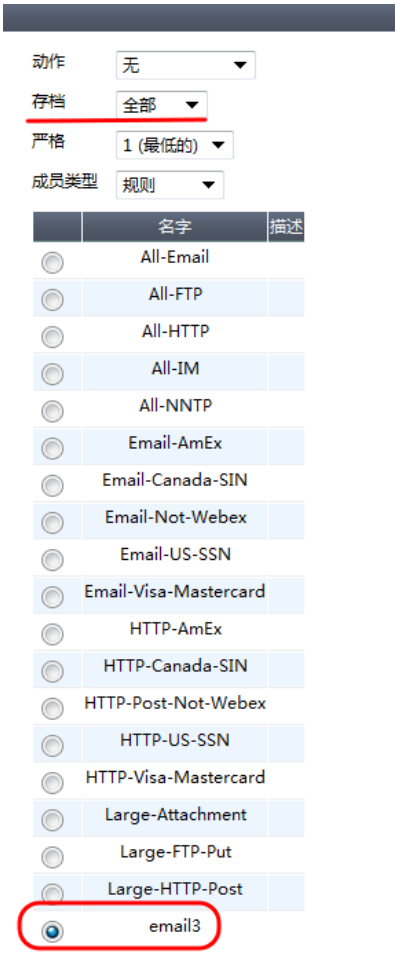
定义多个 dlp 条件,则继续添加 dlp 规则。



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。



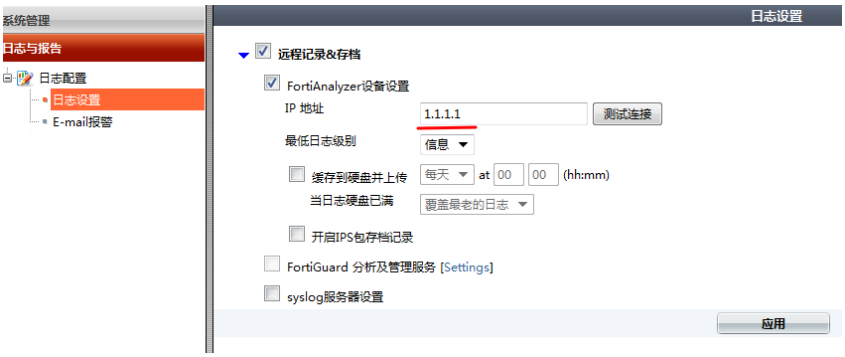
4.3 策略调用 DLP

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。

4.4 定义 FortiAnalyzer

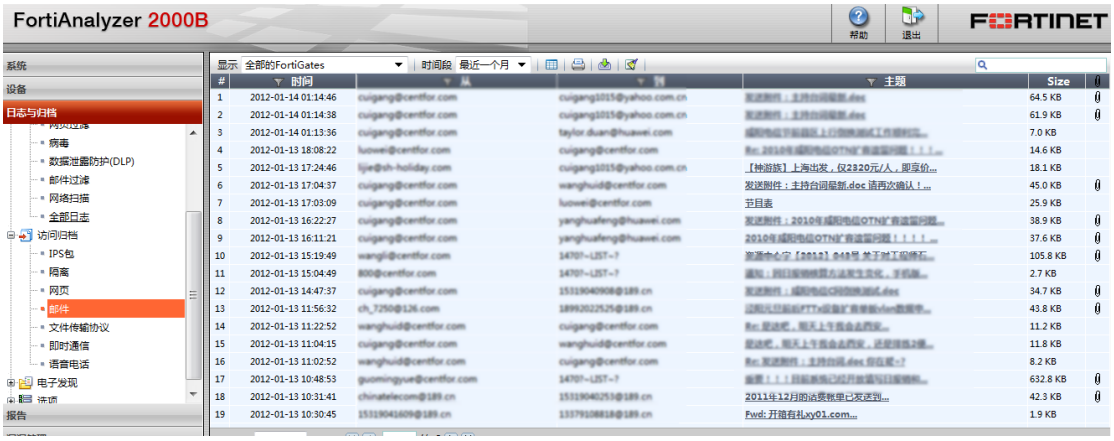
在日志设定中定义日志接收 FortiAnalyzer 地址



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。



6. 参考

UTM

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