FortiWeb 基本配置

版本	1.0
时间	2011 年 9 月
作者	胡丹丹(ddhu@fortinet.com)
支持的版本	FortiWeb v4.3
状态	草稿

目录

1.目的

本文档针对 FortWeb MR3 及以上的在线保护模式和纯粹透明代理模式配置进行说明。FortWeb 支持 4 种模式，各个模式的特点和区别如下:

在线保护(反向代理):反向代理模式下流量将流入虚拟服务器的网络接口和 IP 地址。FortiWeb 会将虚拟服务器接收到的流量转发到物理服务器。FortiWeb 将根据匹配的策略和相应的保护内容表来记录日志,阻断,或修改流量。该模式支持用户认证；

离线保护: FortiWeb 将监控虚拟服务器收到的流量， FortiWeb 将根据匹配的策略和相应的保护内容表来记录日志,阻断流量。如果 FortiWeb 检测到恶意的 HTTP 请求,它将尝试重置该连接。它不修改任何流量。该模式不支持用户认证；

纯粹透明代理：此代理流量将流入物理服务器。流量在 FortiWeb 2 层的网络接口被接收，使用此模式不需要更改用户的网络或服务器地址方案。该模式支持 HTTP 认证(不支持 HTTPS)；

透明检测：此代理流量将流入物理服务器，FortiWeb 对流量进行异步检测，FortiWeb 根据策略或保护内容表对流量进行日志记录或者阻断，不对流量做任何修改，同样不需要更改用户的网络或服务器地址方案，不支持用户认证。

该文中将仅对常用的在线保护模式以及纯粹透明代理模式进行说明。

切换模式时请注意保存原模式配置。

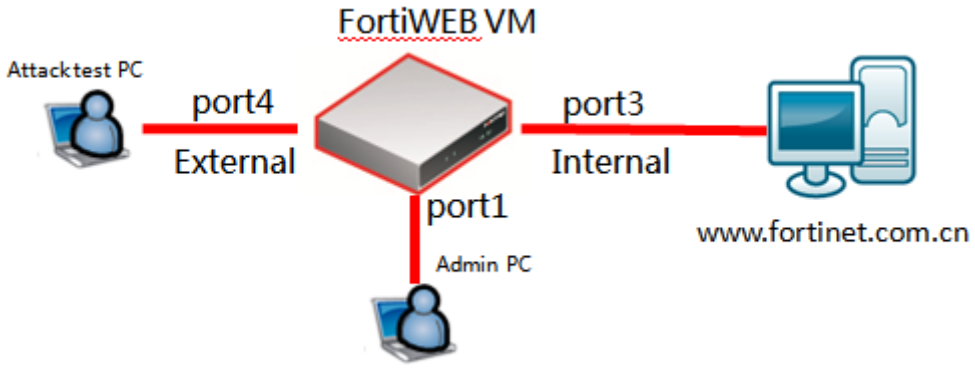
2.环境介绍

本文使用 FortiWeb VM 做演示。本文支持的系统版本为 FortiWeb v4.0MR3 及更高。

出厂设备默认的访问方式是:https、ping、ssh；接口 port1 默认登陆地址:https://192.168.1.99;默认登陆帐号:admin;密码为空。

3.FortiWeb 纯粹透明代理模式配置

本文以 FortiWeb 模拟真实环境，Port4 对应外部接口，Port3 对应内部接口，在实际配置硬件 FortiWeb 可以据此参考。



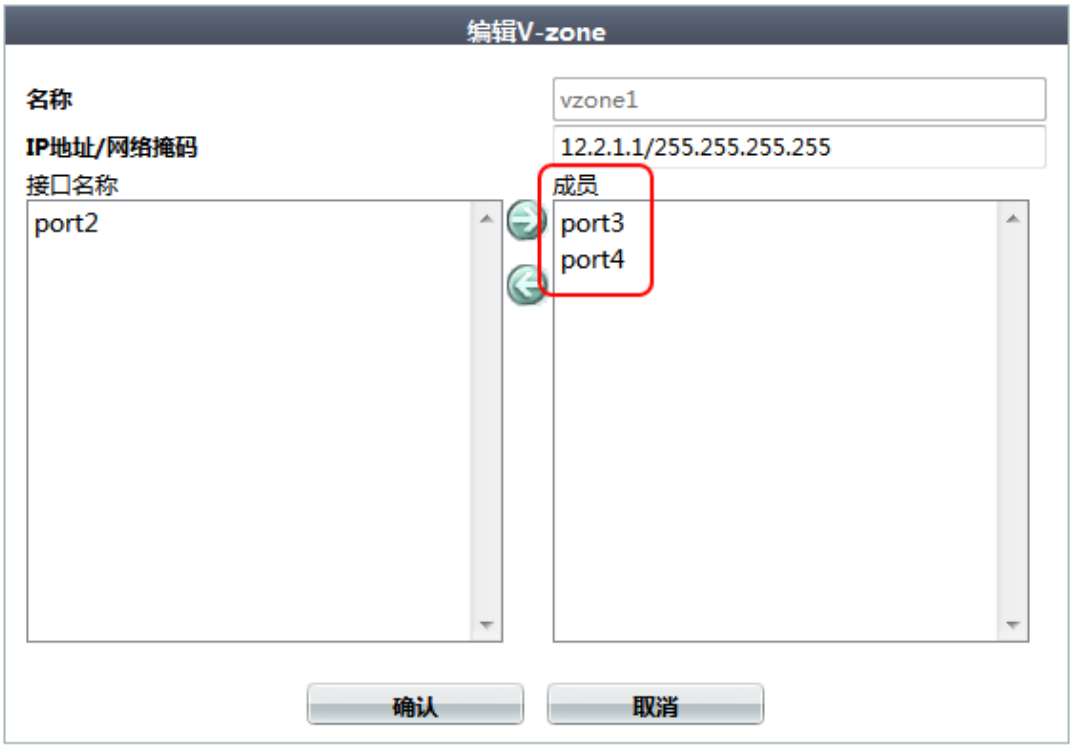
3.1. 启用纯粹透明代理模式

在系统状态中的系统信息将操作模式更改为纯粹透明代理。

3.2. 创建 V-zone 接口

V-zone 是一个虚拟接口，用于桥接 2 个 2 层的网络接口，此例中为 Port3,Port4。

进入系统—网络—V-zone，输入名称，该 V-zone 接口的 IP 地址,此 IP 可以为任意现有网络不冲突的 IP 地址(此地址用于流量检测代理)。成员选择对应的内外网络的两个接口。



3.3. 创建服务器对象

服务器对象—服务器—新建物理服务器

服务器对象—服务器—新建服务器集合

3.4. 创建服务器策略

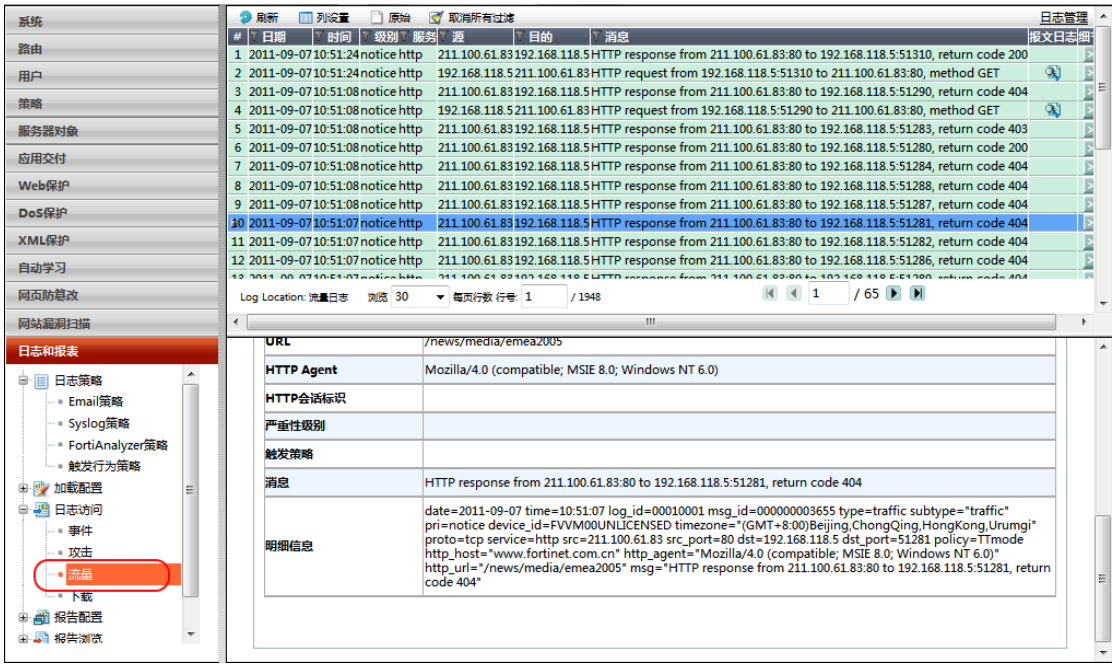
策略—新建服务器策略

至此，纯粹透明代理模式的基本配置就完成了。在完成配置以后，可以通过 Acunetix Web Vulnerability Scanner 或者其他扫描工具对已经被保护的服务器进行扫描，来查看 FortiWeb 是否已经正常工作。

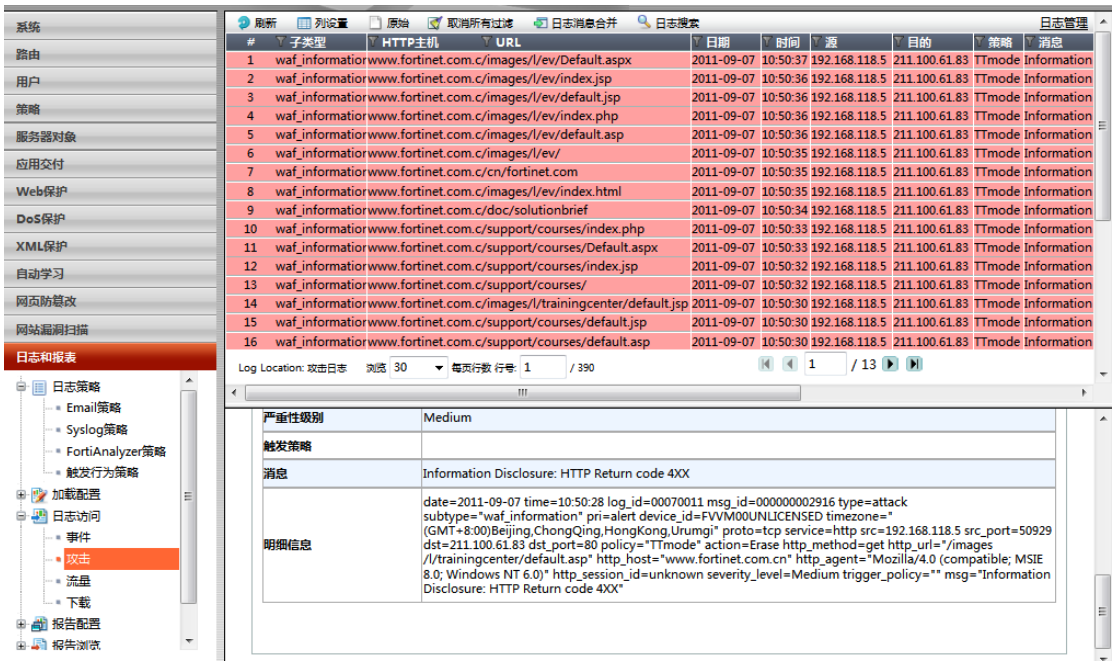
3.5. 查看日志及测试

保护服务器被访问时，流量日志将记录相关信息，当访问流量被检测为攻击类型，该事件将被记录在攻击日志中。通过日志与报告菜单可以查看相关的保护服务器的流量日志以及攻击事件日志来检测配置是否生效。

流量日志



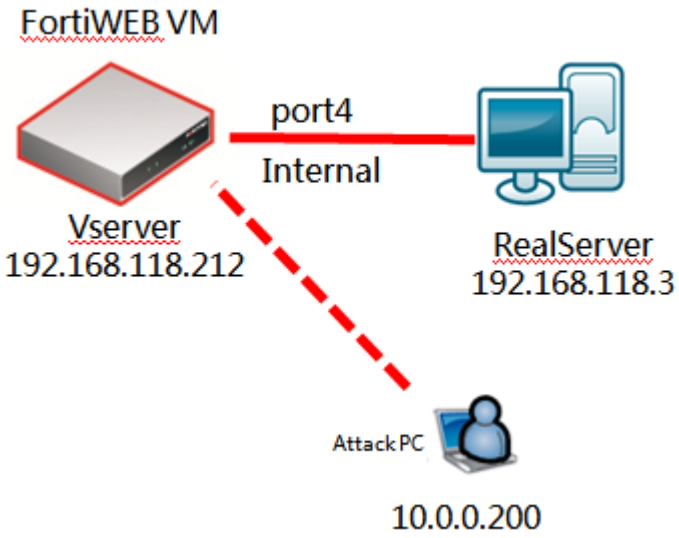
攻击日志



4.在线保护模式配置

FortiWeb 在线保护模式可以单臂模式部署，该文以此模式为例。实验拓

扑结构如下,Port3 对应外部接口，物理服务器的 IP 地址为 192.168.118.3,虚拟服务器的 IP 为 192.168.118.212。外部攻击主机为 10.0.0.200。在实际配置硬件 FortiWeb 可以据此参考。



4.1. 启用在线保护模式

登陆 FortiWeb，在系统状态中的系统信息将操作模式更改为在线保护模式。

4.2. 配置网络接口及路由

单臂模式下，物理服务器的网关为 Port3 接口，可以直接或间接与外网相连

为 FortiWeb 创建路由使其能够访问外网

4.3. 创建服务器对象

服务器对象—服务器—新建物理服务器，此对象为真实服务器

服务器对象—服务器—新建虚拟服务器，此地址为对外发布地址。

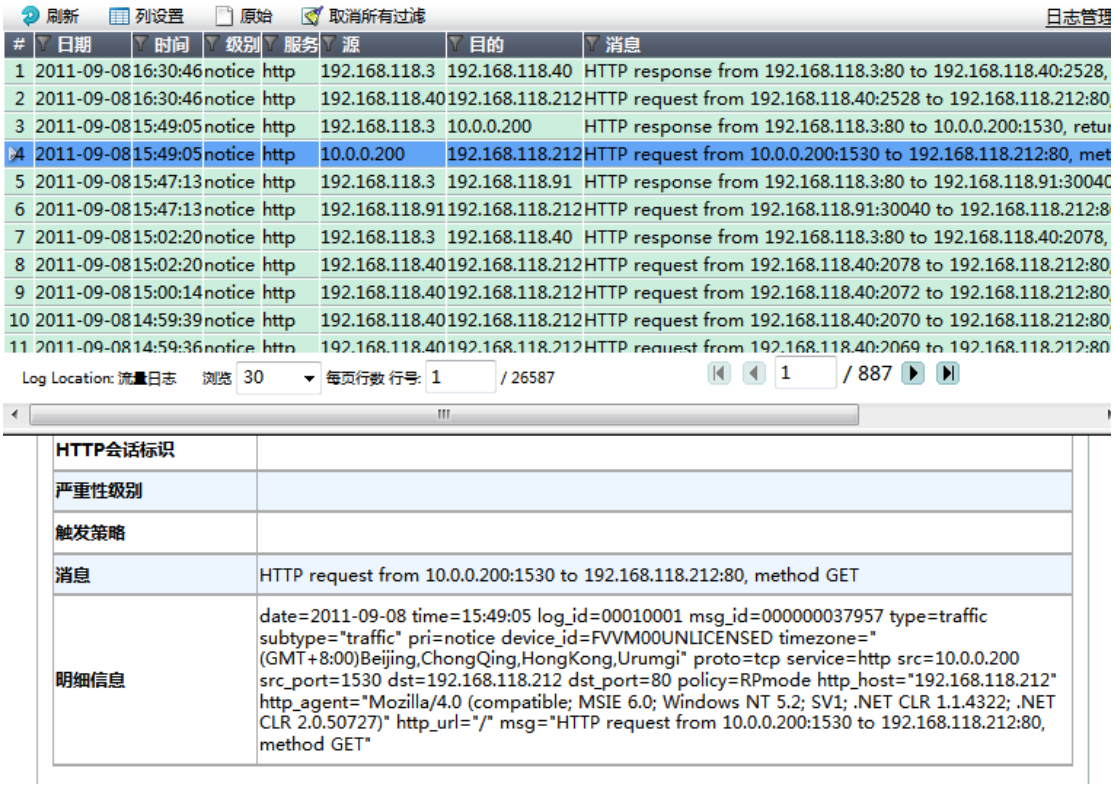
4.4. 创建服务器策略

策略—新建服务器策略

同样，在配置完成后，我们也可以通过纯粹透明代理使用的方法来检查在线保护模式的工作情况。

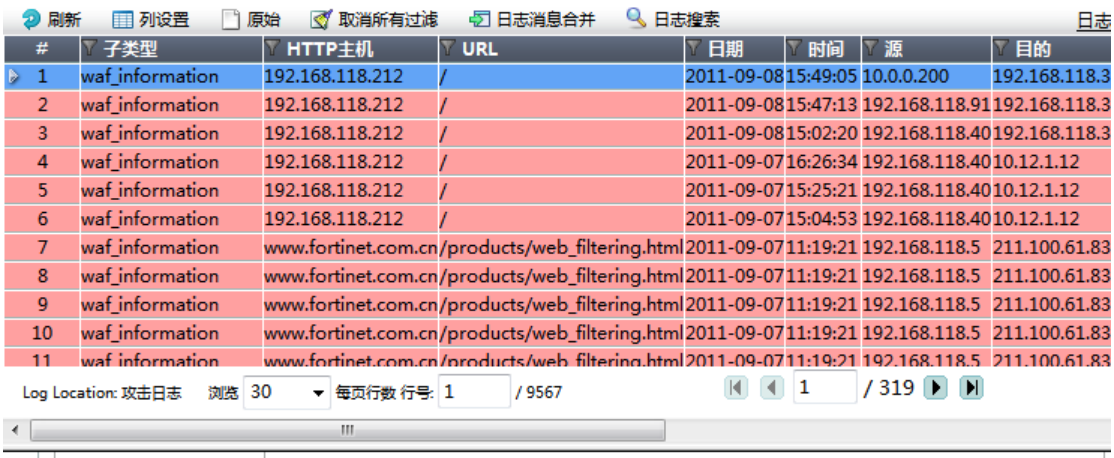
4.5. 查看日志及测试

流量日志



HTTP会话标识	
严重性级别	
触发策略	
消息	HTTP request from 10.0.0.200:1530 to 192.168.118.212:80, method GET
明细信息	date=2011-09-08 time=15:49:05 log_id=00010001 msg_id=000000037957 type=traffic subtype="traffic" pri=notice device_id=FVVM00UNLICENSED timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" proto=tcp service=http src=10.0.0.200 src_port=1530 dst=192.168.118.212 dst_port=80 policy=RPmode http_host="192.168.118.212" http_agent="Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 1.1.4322; .NET CLR 2.0.50727)" http_url="/" msg="HTTP request from 10.0.0.200:1530 to 192.168.118.212:80, method GET"

攻击日志



严重性级别	Medium
触发策略	
消息	Information Disclosure: HTTP Return code 4XX
明细信息	date=2011-09-08 time=15:49:05 log_id=00070011 msg_id=000000037959 type=attack subtype="waf_information" pri=alert device_id=FVVM00UNLICENSED timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" proto=tcp service=http src=10.0.0.200 src_port=1530 dst=192.168.118.3 dst_port=80 policy="RPmode" action=Erase http_method=get http_url="/" http_host="192.168.118.212" http_agent="Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 1.1.4322; .NET CLR 2.0.50727)" http_session_id=unknown severity_level=Medium trigger_policy="" msg="Information Disclosure: HTTP Return code 4XX"

5.查看策略摘要

通过系统状态的策略摘要可以看到 HTTP 访问记录 ,流量信息已经攻击记录