

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	3
2.环境介绍.....	3
3.FortiWeb 纯粹透明代理模式配置	4
3.1. 启用纯粹透明代理模式	4
3.2. 创建 V-zone 接口	5
3.3. 创建服务器对象	5
3.4. 创建服务器策略	6
3.5. 查看日志及测试	7
4.在线保护模式配置	8
4.1. 启用在线保护模式	9
4.2. 配置网络接口及路由	9
4.3. 创建服务器对象	10
4.4. 创建服务器策略	11
4.5. 查看日志及测试	11
5.查看策略摘要	13

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。

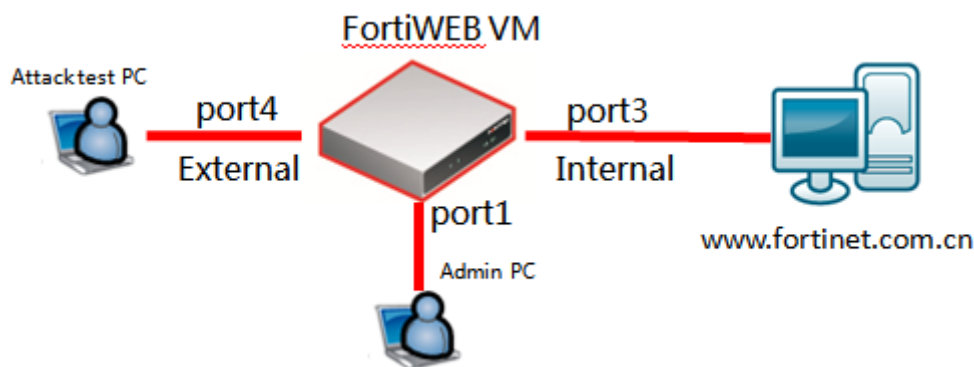
2.环境介绍

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。

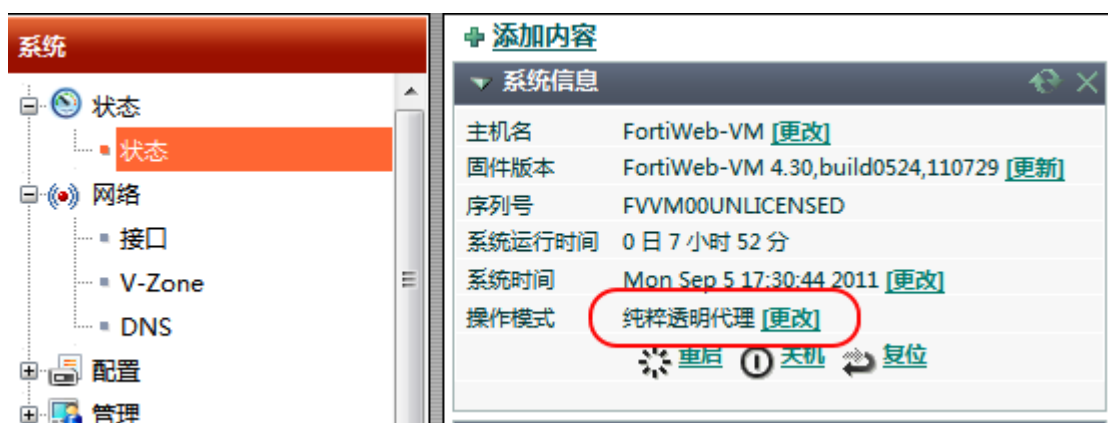
3.FortiWeb 纯粹透明代理模式配置

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

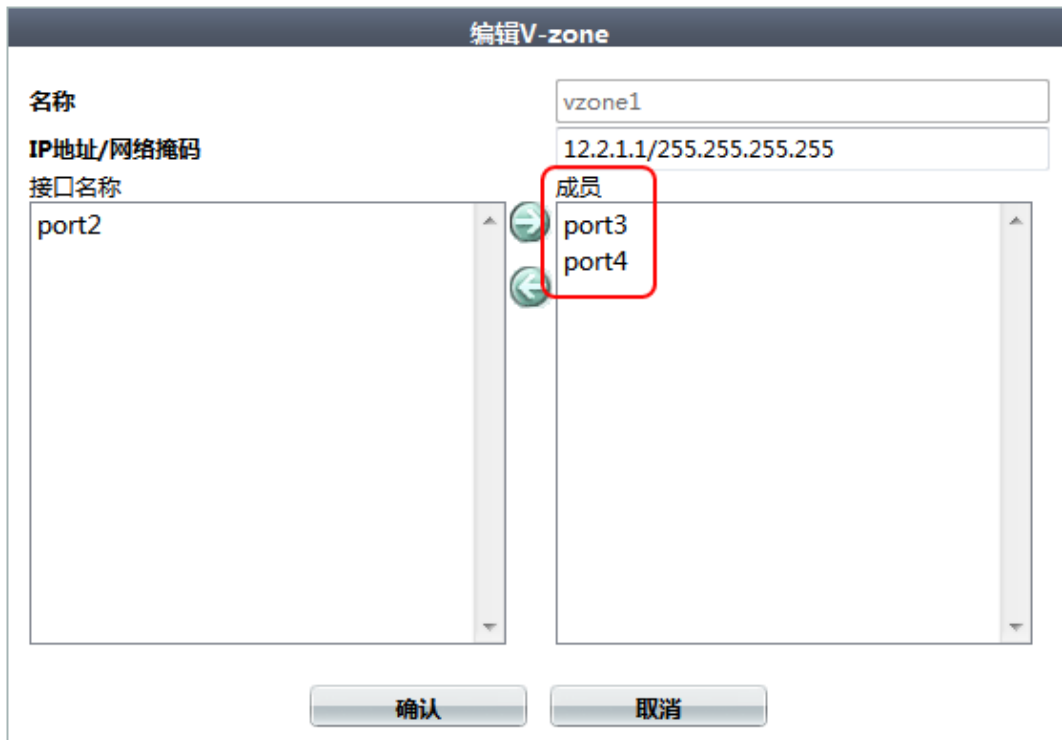
在系统状态中的系统信息将操作模式更改为纯粹透明代理。



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

编辑物理服务器

名称

IP地址

服务器对象—服务器—新建服务器集合

编辑服务器集合

服务器集合名称

注释

服务器类型

- 服务器均衡
- WSDL内容路由
- HTTP内容路由
- XML内容路由
- 透明服务器
- 离线保护

ID	服务器	端口	SSL	证书	
1	www.fortinet.com.cn	80	禁用		

3.4. 创建服务器策略

策略—新建服务器策略

编辑策略

策略名称	<input type="text" value="TTmode"/>
策略类型	Web保护 ▾
模式	透明服务器 ▾
V-Zone	vzone1 ▾
服务器集合	TTserver ▾
被保护服务器	[选择...] ▾
持续的服务器会话	<input type="text" value="1000"/> (1000~8000)

Syn Cookie	<input type="checkbox"/>
最大半开连接数	<input type="text" value="100"/>

Web保护规范	Inline High Level Security ▾
	<input type="button" value="查看保护规范细节"/>
WAF自学习规范	Default Auto Learn Profile ▾
监视模式	<input type="checkbox"/>
URL大小写敏感	<input type="checkbox"/>
错误页面策略	[选择...] ▾

注释 (最大35个字符)

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

The screenshot shows the Fortinet traffic log interface. On the left is a navigation menu with '日志和报表' (Logs and Reports) selected, and '流量' (Traffic) highlighted. The main area displays a table of log entries:

#	日期	时间	级别	服务	源	目的	消息
1	2011-09-07	10:51:24	notice	http	211.100.61.83	192.168.118.5	HTTP response from 211.100.61.83:80 to 192.168.118.5:51310, return code 200
2	2011-09-07	10:51:24	notice	http	192.168.118.5	211.100.61.83	HTTP request from 192.168.118.5:51310 to 211.100.61.83:80, method GET
3	2011-09-07	10:51:08	notice	http	211.100.61.83	192.168.118.5	HTTP response from 211.100.61.83:80 to 192.168.118.5:51290, return code 404
4	2011-09-07	10:51:08	notice	http	192.168.118.5	211.100.61.83	HTTP request from 192.168.118.5:51290 to 211.100.61.83:80, method GET
5	2011-09-07	10:51:08	notice	http	211.100.61.83	192.168.118.5	HTTP response from 211.100.61.83:80 to 192.168.118.5:51283, return code 403
6	2011-09-07	10:51:08	notice	http	211.100.61.83	192.168.118.5	HTTP response from 211.100.61.83:80 to 192.168.118.5:51280, return code 200
7	2011-09-07	10:51:08	notice	http	211.100.61.83	192.168.118.5	HTTP response from 211.100.61.83:80 to 192.168.118.5:51284, return code 404
8	2011-09-07	10:51:08	notice	http	211.100.61.83	192.168.118.5	HTTP response from 211.100.61.83:80 to 192.168.118.5:51288, return code 404
9	2011-09-07	10:51:08	notice	http	211.100.61.83	192.168.118.5	HTTP response from 211.100.61.83:80 to 192.168.118.5:51287, return code 404
10	2011-09-07	10:51:07	notice	http	211.100.61.83	192.168.118.5	HTTP response from 211.100.61.83:80 to 192.168.118.5:51281, return code 404
11	2011-09-07	10:51:07	notice	http	211.100.61.83	192.168.118.5	HTTP response from 211.100.61.83:80 to 192.168.118.5:51282, return code 404
12	2011-09-07	10:51:07	notice	http	211.100.61.83	192.168.118.5	HTTP response from 211.100.61.83:80 to 192.168.118.5:51286, return code 404

The detailed view for entry 10 shows:

- URL: /news/media/emea2005
- HTTP Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0)
- HTTP会话标识: (empty)
- 严重性级别: (empty)
- 触发策略: (empty)
- 消息: HTTP response from 211.100.61.83:80 to 192.168.118.5:51281, return code 404
- 明细信息: date=2011-09-07 time=10:51:07 log_id=00010001 msg_id=00000003655 type=traffic subtype="traffic" pri=notice device_id=FVVM00UNLICENSED timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumqi" proto=tcp service=http src=211.100.61.83 src_port=80 dst=192.168.118.5 dst_port=51281 policy=TTmode http_host="www.fortinet.com.cn" http_agent="Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0)" http_url="/news/media/emea2005" msg="HTTP response from 211.100.61.83:80 to 192.168.118.5:51281, return code 404"

攻击日志

The screenshot shows the Fortinet attack log interface. On the left is a navigation menu with '日志和报表' (Logs and Reports) selected, and '攻击' (Attack) highlighted. The main area displays a table of log entries:

#	子类型	HTTP主机	URL	日期	时间	源	目的	策略	消息
1	waf_informator	www.fortinet.com	/images/l/ev/Default.aspx	2011-09-07	10:50:37	192.168.118.5	211.100.61.83	TTmode	Information
2	waf_informator	www.fortinet.com	/images/l/ev/index.jsp	2011-09-07	10:50:36	192.168.118.5	211.100.61.83	TTmode	Information
3	waf_informator	www.fortinet.com	/images/l/ev/default.jsp	2011-09-07	10:50:36	192.168.118.5	211.100.61.83	TTmode	Information
4	waf_informator	www.fortinet.com	/images/l/ev/index.php	2011-09-07	10:50:36	192.168.118.5	211.100.61.83	TTmode	Information
5	waf_informator	www.fortinet.com	/images/l/ev/default.asp	2011-09-07	10:50:36	192.168.118.5	211.100.61.83	TTmode	Information
6	waf_informator	www.fortinet.com	/images/l/ev/	2011-09-07	10:50:35	192.168.118.5	211.100.61.83	TTmode	Information
7	waf_informator	www.fortinet.com	/cn/fortinet.com	2011-09-07	10:50:35	192.168.118.5	211.100.61.83	TTmode	Information
8	waf_informator	www.fortinet.com	/images/l/ev/index.html	2011-09-07	10:50:35	192.168.118.5	211.100.61.83	TTmode	Information
9	waf_informator	www.fortinet.com	/doc/solutionbrief	2011-09-07	10:50:34	192.168.118.5	211.100.61.83	TTmode	Information
10	waf_informator	www.fortinet.com	/support/courses/index.php	2011-09-07	10:50:33	192.168.118.5	211.100.61.83	TTmode	Information
11	waf_informator	www.fortinet.com	/support/courses/Default.aspx	2011-09-07	10:50:33	192.168.118.5	211.100.61.83	TTmode	Information
12	waf_informator	www.fortinet.com	/support/courses/index.jsp	2011-09-07	10:50:32	192.168.118.5	211.100.61.83	TTmode	Information
13	waf_informator	www.fortinet.com	/support/courses/	2011-09-07	10:50:32	192.168.118.5	211.100.61.83	TTmode	Information
14	waf_informator	www.fortinet.com	/images/l/trainingcenter/default.jsp	2011-09-07	10:50:30	192.168.118.5	211.100.61.83	TTmode	Information
15	waf_informator	www.fortinet.com	/support/courses/default.jsp	2011-09-07	10:50:30	192.168.118.5	211.100.61.83	TTmode	Information
16	waf_informator	www.fortinet.com	/support/courses/default.asp	2011-09-07	10:50:30	192.168.118.5	211.100.61.83	TTmode	Information

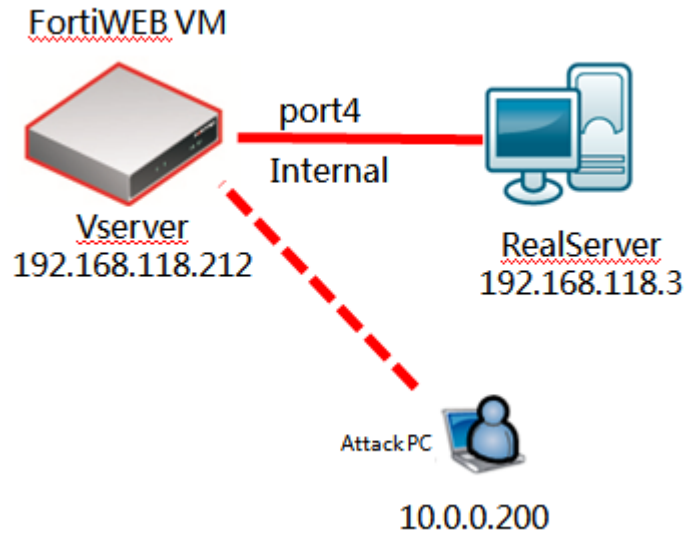
The detailed view for entry 16 shows:

- 严重性级别: Medium
- 触发策略: (empty)
- 消息: Information Disclosure: HTTP Return code 4XX
- 明细信息: date=2011-09-07 time=10:50:28 log_id=00070011 msg_id=00000002916 type=attack subtype="waf_informator" pri=alert device_id=FVVM00UNLICENSED timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumqi" proto=tcp service=http src=192.168.118.5 src_port=50929 dst=211.100.61.83 dst_port=80 policy="TTmode" action=Eraser http_method=get http_url="/images/l/trainingcenter/default.asp" http_host="www.fortinet.com.cn" http_agent="Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0)" http_session_id="unknown severity_level=Medium trigger_policy="" msg="Information Disclosure: HTTP Return code 4XX"

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

#	名称	IP地址 / 网络掩码	访问选项	状态
<input type="checkbox"/>	port1	192.168.1.99 / 255.255.255.0	HTTPS,PING,SSH,SNMP,HTTP,TELNET	关闭
<input type="checkbox"/>	port2	0.0.0.0 / 0.0.0.0		关闭
<input type="checkbox"/>	port3	192.168.118.23 / 255.255.255.0	HTTPS,PING,HTTP	关闭
<input type="checkbox"/>	port4	0.0.0.0 / 0.0.0.0	HTTPS,PING,SSH,SNMP,HTTP	关闭

为 FortiWeb 创建路由使其能够访问外网

编辑路由

目的 IP/掩码

网关

接口

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

编辑物理服务器

名称

IP地址

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。

编辑虚拟服务器

名称

IP地址

接口

4.4. 创建服务器策略

策略—新建服务器策略

编辑策略	
策略名称	RPmode
策略类型	Web保护
模式	单服务器
虚拟服务器	Vserver
服务器类型	<input checked="" type="radio"/> 物理服务器 <input type="radio"/> 域名服务器
物理服务器	testserver
被保护服务器	[选择...]
持续的服务器会话	1000 (1000~8000)
<hr/>	
HTTP服务	HTTP
物理服务器端口	80 (1 ~ 65535)
<hr/>	
HTTPS服务	[选择...]
<hr/>	
Web保护规范	Inline Medium Level Security
	查看保护规范细节
WAF自学习规范	[选择...]
监视模式	<input type="checkbox"/>
URL大小写敏感	<input type="checkbox"/>
错误页面策略	[选择...]

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

刷新 列表设置 原始 取消所有过滤 日志管理

#	日期	时间	级别	服务	源	目的	消息
1	2011-09-08	16:30:46	notice	http	192.168.118.3	192.168.118.40	HTTP response from 192.168.118.3:80 to 192.168.118.40:2528,
2	2011-09-08	16:30:46	notice	http	192.168.118.40	192.168.118.212	HTTP request from 192.168.118.40:2528 to 192.168.118.212:80
3	2011-09-08	15:49:05	notice	http	192.168.118.3	10.0.0.200	HTTP response from 192.168.118.3:80 to 10.0.0.200:1530, retur
4	2011-09-08	15:49:05	notice	http	10.0.0.200	192.168.118.212	HTTP request from 10.0.0.200:1530 to 192.168.118.212:80, met
5	2011-09-08	15:47:13	notice	http	192.168.118.3	192.168.118.91	HTTP response from 192.168.118.3:80 to 192.168.118.91:30040
6	2011-09-08	15:47:13	notice	http	192.168.118.91	192.168.118.212	HTTP request from 192.168.118.91:30040 to 192.168.118.212:8
7	2011-09-08	15:02:20	notice	http	192.168.118.3	192.168.118.40	HTTP response from 192.168.118.3:80 to 192.168.118.40:2078,
8	2011-09-08	15:02:20	notice	http	192.168.118.40	192.168.118.212	HTTP request from 192.168.118.40:2078 to 192.168.118.212:80
9	2011-09-08	15:00:14	notice	http	192.168.118.40	192.168.118.212	HTTP request from 192.168.118.40:2072 to 192.168.118.212:80
10	2011-09-08	14:59:39	notice	http	192.168.118.40	192.168.118.212	HTTP request from 192.168.118.40:2070 to 192.168.118.212:80
11	2011-09-08	14:59:36	notice	http	192.168.118.40	192.168.118.212	HTTP request from 192.168.118.40:2069 to 192.168.118.212:80

Log Location: 流量日志 浏览 30 每页行数 行号: 1 / 26587 1 / 887

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

刷新 列表设置 原始 取消所有过滤 日志消息合并 日志搜索 日志

#	子类型	HTTP主机	URL	日期	时间	源	目的
1	waf_information	192.168.118.212	/	2011-09-08	15:49:05	10.0.0.200	192.168.118.3
2	waf_information	192.168.118.212	/	2011-09-08	15:47:13	192.168.118.91	192.168.118.3
3	waf_information	192.168.118.212	/	2011-09-08	15:02:20	192.168.118.40	192.168.118.3
4	waf_information	192.168.118.212	/	2011-09-07	16:26:34	192.168.118.40	10.12.1.12
5	waf_information	192.168.118.212	/	2011-09-07	15:25:21	192.168.118.40	10.12.1.12
6	waf_information	192.168.118.212	/	2011-09-07	15:04:53	192.168.118.40	10.12.1.12
7	waf_information	www.fortinet.com.cn	/products/web_filtering.html	2011-09-07	11:19:21	192.168.118.5	211.100.61.83
8	waf_information	www.fortinet.com.cn	/products/web_filtering.html	2011-09-07	11:19:21	192.168.118.5	211.100.61.83
9	waf_information	www.fortinet.com.cn	/products/web_filtering.html	2011-09-07	11:19:21	192.168.118.5	211.100.61.83
10	waf_information	www.fortinet.com.cn	/products/web_filtering.html	2011-09-07	11:19:21	192.168.118.5	211.100.61.83
11	waf_information	www.fortinet.com.cn	/products/web_filtering.html	2011-09-07	11:19:21	192.168.118.5	211.100.61.83

Log Location: 攻击日志 浏览 30 每页行数 行号: 1 / 9567 1 / 319

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

