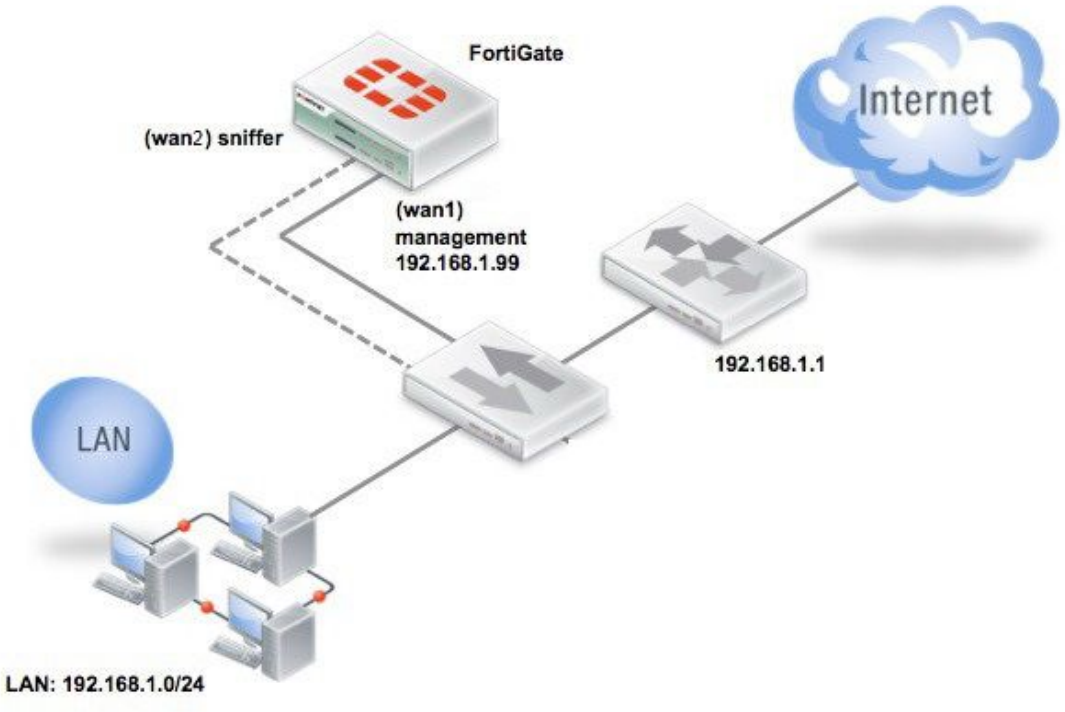
防火墙单臂离线分析网络流量

版本	1.0
时间	2014 年 11 月
支持的版本	FortiOS v5.2 及更高版本
审核	已通过
反馈	support_cn@fortinet.com

目录

内容一：拓扑介绍



本文档介绍防火墙离线单臂嗅探部署模式，FOS 要使用 5.2 版本。在拓扑中将相关流量通过交换机的端口镜像功能发送给防火墙，防火墙可以分析出流量、反病毒、IPS、网址和应用类型日志。

内容二：在交换机上配置端口镜像

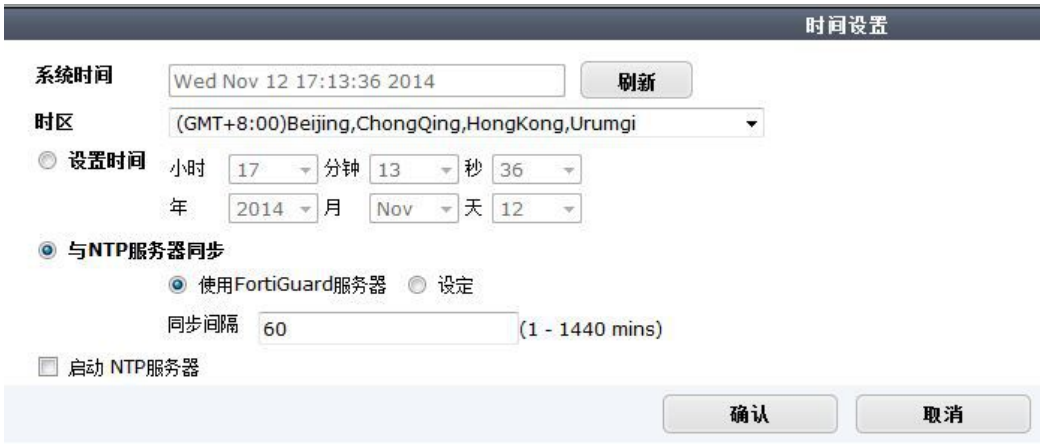
以 CISCO 交换机配置为例：

monitor session 1 source vlan 5 , 6

monitor session 1 destination interface Gi0/23

内容三：配置好时间和时区

确保使用正确的时间和时区



内容四：确保使用最新反病毒，IPS 特征库

防火墙要使用最新的反病毒和 IPS 库，确保有 fortiguard 服务。

在系统管理—>配置—>FortiGuard 菜单中查看反病毒和 IPS 库版本

内容五：配置接口嗅探模式

在系统管理→网络→接口 菜单下修改 wan2 接口为单臂嗅探模式，启用反病毒、网页过滤、应用控制和 IPS 监控选项，记录所有日志

对应的 CLI，

```
config system interface
    edit "wan2"
        set vdom "root"
        set allowaccess ping
        set ips-sniffer-mode enable
        set type physical
        set snmp-index 3
    next
end
config firewall sniffer
    edit 1
        set logtraffic all
        set interface "wan2"
        set application-list-status enable
        set application-list "default"
        set ips-sensor-status enable
        set ips-sensor "all_default_pass"
        set av-profile-status enable
        set av-profile "AV-flow"
        set webfilter-profile-status enable
        set webfilter-profile "flow-monitor-all"
    next
end
```

内容六：配置 UTM

在 CLI 下调整 UTM 内容表，

1， 在页面上显示多个 UTM 内容表

```
config system global
   set gui-multiple-utm-profiles enable
end
```

2， 修改应用控制内容表

```
config application list
      edit "default"
            set other-application-log enable
end
```

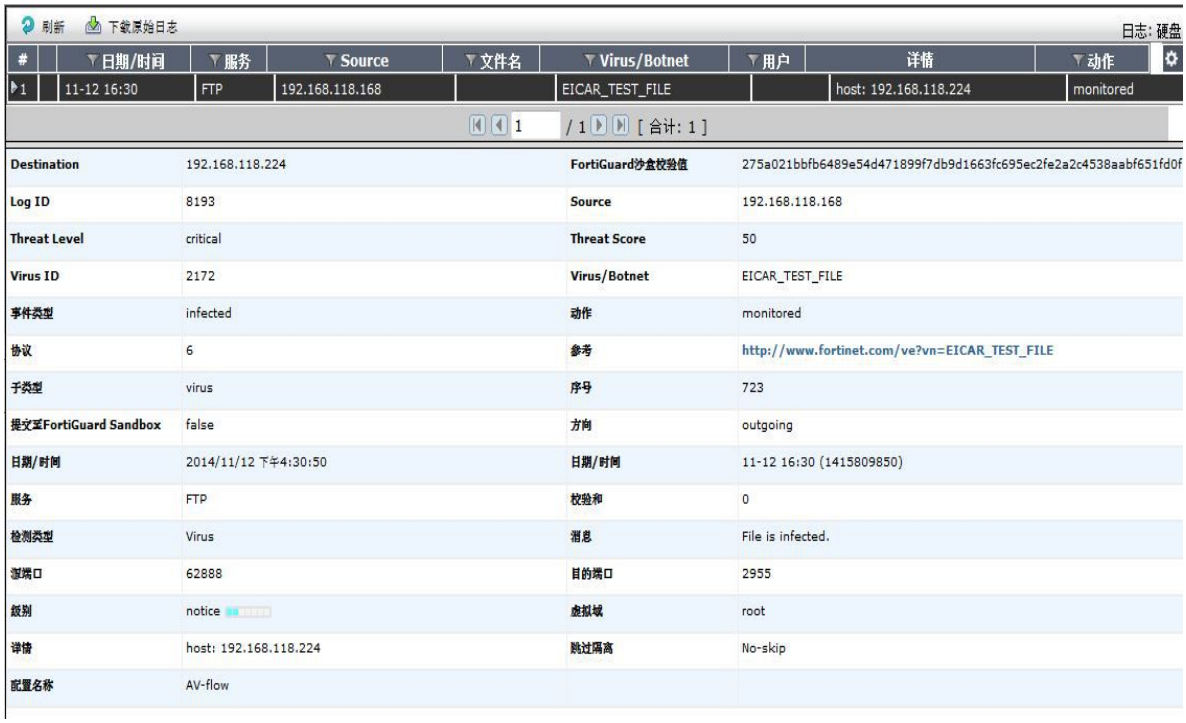
3， 修改 IPS 内容表

```
config ips sensor
      edit "all_default_pass"
                  config entries
                        edit 1
                              set status enable
                        next
                  end
      next
end
```

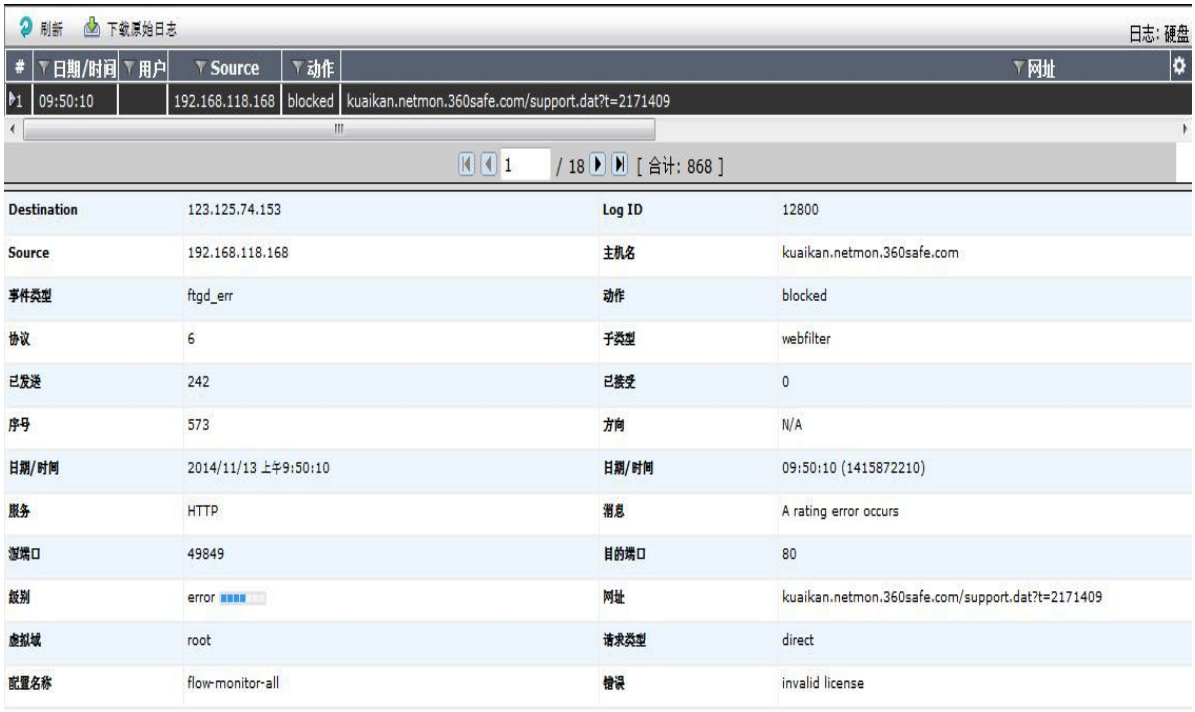
内容七：查看监控日志

流量日志：

反病毒日志：



网页过滤日志：

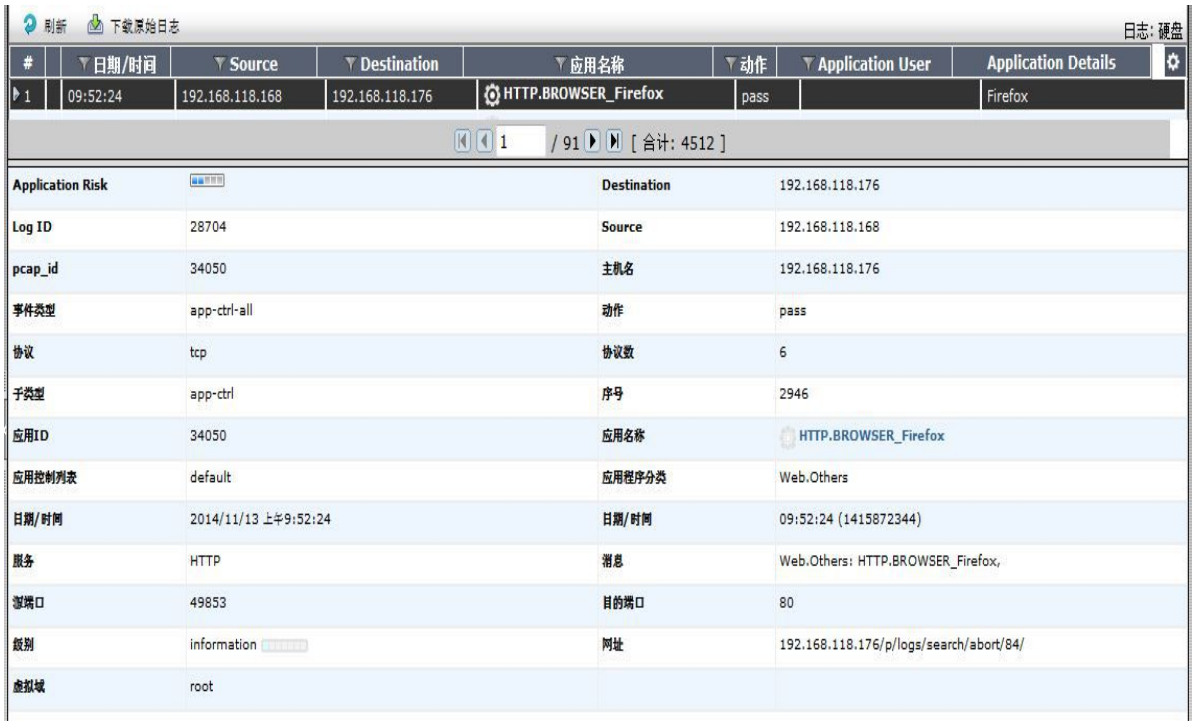

刷新 下载原始日志 日志: 硬盘

#	日期/时间	用户	Source	动作	网址
1	09:50:10		192.168.118.168	blocked	kuaikan.netmon.360safe.com/support.dat?t=2171409

1 / 18 [合计: 868]

Destination	123.125.74.153	Log ID	12800
Source	192.168.118.168	主机名	kuaikan.netmon.360safe.com
事件类型	ftgd_err	动作	blocked
协议	6	子类型	webfilter
已发送	242	已接受	0
序号	573	方向	N/A
日期/时间	2014/11/13 上午9:50:10	日期/时间	09:50:10 (1415872210)
服务	HTTP	消息	A rating error occurs
源端口	49849	目的端口	80
级别	error	网址	kuaikan.netmon.360safe.com/support.dat?t=2171409
虚拟域	root	请求类型	direct
配置名称	flow-monitor-all	错误	invalid license

应用控制日志：


刷新 下载原始日志 日志: 硬盘

#	日期/时间	Source	Destination	应用名称	动作	Application User	Application Details
1	09:52:24	192.168.118.168	192.168.118.176	HTTP.BROWSER_Firefox	pass		Firefox

1 / 91 [合计: 4512]

Application Risk		Destination	192.168.118.176
Log ID	28704	Source	192.168.118.168
pcap_id	34050	主机名	192.168.118.176
事件类型	app-ctrl-all	动作	pass
协议	tcp	协议数	6
子类型	app-ctrl	序号	2946
应用ID	34050	应用名称	HTTP.BROWSER_Firefox
应用控制列表	default	应用程序分类	Web.Others
日期/时间	2014/11/13 上午9:52:24	日期/时间	09:52:24 (1415872344)
服务	HTTP	消息	Web.Others: HTTP.BROWSER_Firefox,
源端口	49853	目的端口	80
级别	information	网址	192.168.118.176/p/logs/search/abort/84/
虚拟域	root		

IPS 日志：


刷新 下载原始日志 日志: 硬盘

#		日期/时间	严重性	Source	协议	用户	动作	计数	攻击名称
1		11-12 16:30		192.168.118.168	tcp		detected		Eicar.Virus.Test.File
2		11-12 16:27		192.168.118.168	tcp		detected		Telnet.Login.XSS

1 / 1 [合计: 4]

Destination	192.168.90.117	Log ID	16384
Source	192.168.118.168	Threat Level	medium
Threat Score	10	pcap_id	14288
严重性	medium	事件序列号	848221385
事件类型	signature	动作	detected
协议	tcp	协议数	6
参考	http://www.fortinet.com/ids/VID14288	子类型	ips
序号	100	攻击ID	14288
攻击名称	Telnet.Login.XSS	方向	0
日期/时间	2014/11/12 下午4:27:59	日期/时间	11-12 16:27 (1415809679)
服务	TELNET	消息	remote_access: Telnet.Login.XSS,
源端口	62863	目的端口	23
级别	alert	虚拟域	root
配置名称	all_default_pass		