神州数码

DCFW-1800-WAF产品快速配置

唐进元
tangjya@digitalchina.com

—网络创造价值—

- 初次配置
- 功能配置
- 对象管理
- 状态监控
- 日志报表
- 系统维护
- 其他配置

初次配置

1、确定WAF设备接入电源，按设备后面的电源开关启动设备。

2、网口介绍：WAN口(ETH0)（接Internet或者外网出口设备）

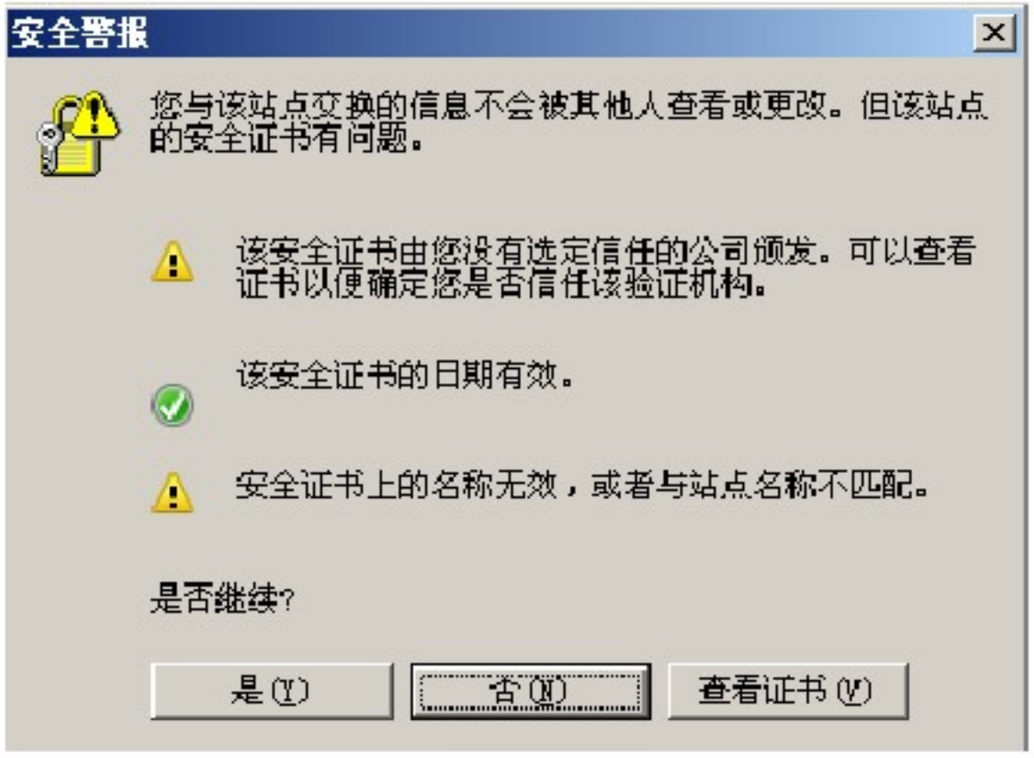
LAN口(ETH1)（接WEB服务器主机）

管理口(ETH5)（用于进行设备管理，可根据需要接入内网交换机）

带外口(ETH4)（用于初次配置WAF设备使用，该端口默认IP为：192.168.45.1 且不能配置更改）

3、打开浏览器IE，用HTTPS方式连接WAF的带外口IP地址：https://192.168.45.1。

4、回车后出现如图所示界面，单击【是】，接受WAF证书加密的通道。



初次配置

初次配置

成功登录后，进入Web管理界面。

初次配置

➢ 网络配置

网络配置界面提供了网络设备的配置接口，请根据实际网络情况配置设备的网络参数。

1、透明模式：配置WAN口IP地址与WEB服务器地址为同一网段，管理口地址根据网络情况进行配置。

2、反向代理模式：WAN口配置为原服务器的IP，LAN口地址的IP配置与WEB服务器同一网段地址，管理口地址根据网络情况进行配置。

3、高级网络配置适用于复杂网络环境，具体配置请参照用户手册。

功能配置-服务管理

DCN | 神州数码 Digital China

- 首页
- 系统
- 配置
- 站点
  - 站点管理
  - 主机状态
  - 应用状态
- 对象
- 检测
- 防护
- 站点加速
- 日志
- 报表

以下是透明模式下配置：

1、服务名称（需要符合规范）

2、服务类型选择，http或者https

3、WEB主机地址及端口

4、策略集，目前有审计（只记录日志）和阻止（记录日志并阻断攻击）

5、域名，同IP端口下可输入多域名

注意：添加服务为重要操作，需准确输入，并等待一个服务添加完成再添加下一个

功能配置-服务管理

DCN | 神州数码 Digital China

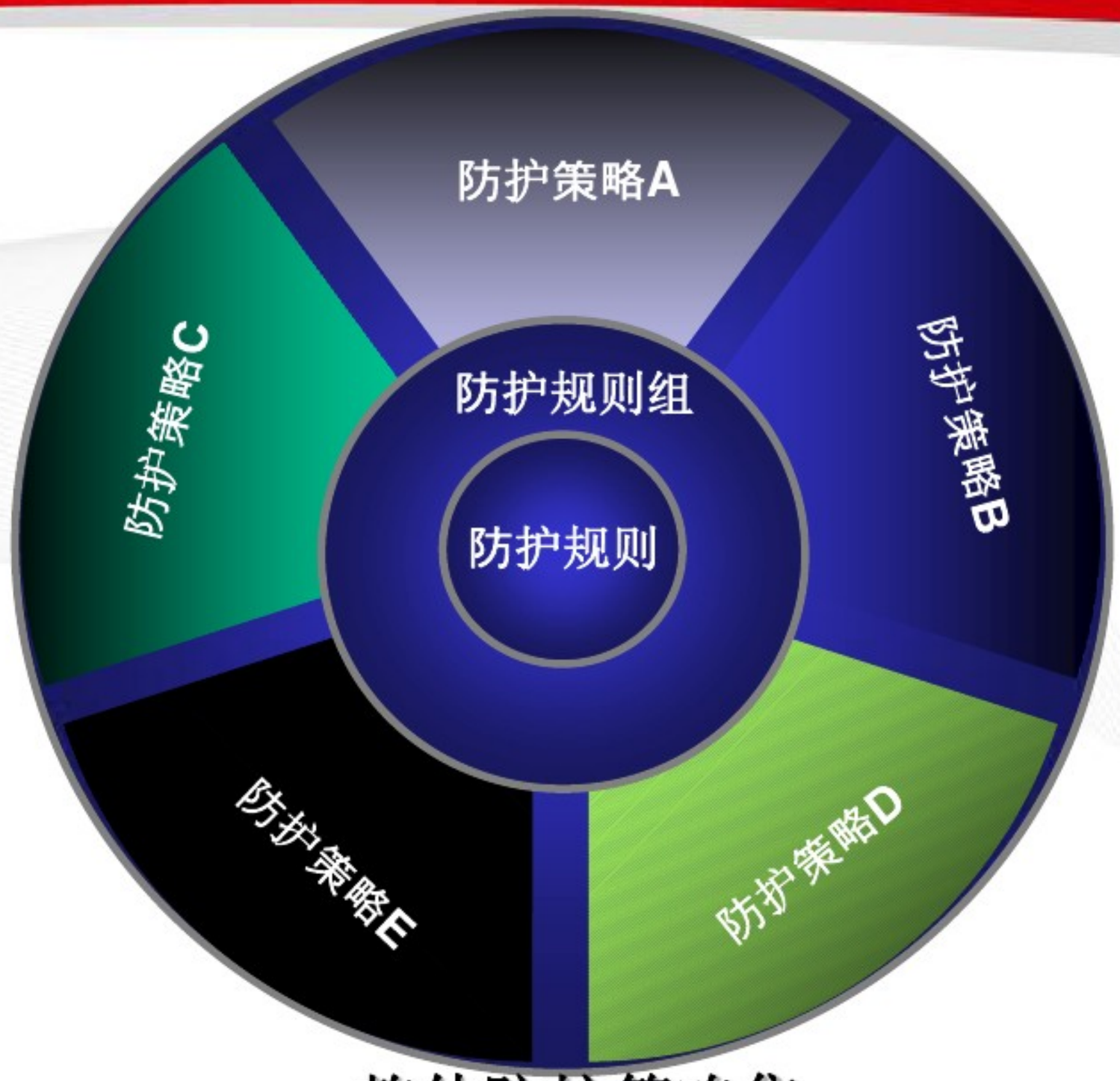
新建服务

*服务名称	字母开头，字母、数字和下划线组成，长度为1到20
*服务类型	HTTP
*主机地址	点分十进制整数，形如：192.168.23.4
*主机端口	1到65535之间的整数
策略集	无
站点域名	添加
站点域名列表	删除选中站点 每行为一个站点的所有域名，输入多个域名，以逗号分隔 ，
*记录访问日志：	是 否

功能配置-WEB攻击防护配置

- 防护规则及策略配置：

1、新建一条防护规则a
2、新建一个防护规则组b
3、将防护规则a加入到防护规则组b中
4、新建一条防护策略c，将防护规则组b加入到防护策略c中
5、新建一条整体防护策略集d，将防护策略c加入到整体防护策略集d中
6、在服务管理中应用整体防护策略集d



整体防护策略集

功能配置-WEB攻击防护配置

- CC防护、盗链防护、请求限制、错误过滤配置说明：

1、新建一条防护策略a

2、新建一条整体防护策略集b（可以使用已存在的整体防护策略集，若没有可新建），将防护策略a应用到整体防护策略集b

3、在服务管理中应用整体防护策略集b

Web防护策略 | CC防护策略 | 盗链防护策略 | 爬虫防护策略 | 扫描防护策略 | 请求限制策略 | 错误过滤策略

策略集编辑：b

防护模块	策略名称	描述	是否加入策略集
请求限制防护	关闭请求限制检测	停止请求限制检测功能，用于调试、排除网络问题。	○
	严格请求限制	根据网站资源和用户访问情况，配置请求限制	○
	中等请求限制	根据网站资源和用户访问情况，配置请求限制	○
	宽松请求限制	根据网站资源和用户访问情况，配置请求限制	○
	zn		○
	a	a	◉

功能配置-DDoS防护配置

- **DDoS攻击防护配置：**

1、点击开启**DDOS**攻击防护按钮即可

2、如不了解网络流量情况可配置参数自学习，并将学习的结果整理后应用到配置中

功能配置-网页防篡改配置

- 防篡改配置：

1、进行配置与初始化操作

2、开启防篡改保护

3、WEB服务器更新页面后要进行镜像同步操作

功能配置-检测配置

- 漏洞扫描配置：

  建立漏洞扫描任务，按要求填入相应项目，对保护服务进行漏洞检测

漏洞扫描管理　　每页显示 10 条，当前第1/1页 [1]

新建...　任务名称：　扫描目标：　查询

序号	选择	任务名称	任务类型	扫描目标	执行时间	当前状态	操作
1	☐	s120	立即执行	192.168.1.225:80	2011-01-27 15:00:24	扫描完成	

全选 ☐　删除所选任务

- 关键字统计配置：

  建立关键字统计任务，按要求填入相应项目，对保护服务进行关键字统计

关键字统计　　每页显示 10 条，当前第1/1页 [1]

新建...　任务名称：所有任务　统计目标名称：请选择统计目标　查询

任务名称	任务类型	统计目标	当前状态	执行方式	执行时间/周期	执行	操作
a120	单任务	192.168.1.195:80	未执行	立即执行	--		

对象管理

- 基本配置方法：

1、新建一个对象a

2、根据需要把对象a加入到对象组中

源IP地址组

新建...

序号	名称	描述	地址段	操作
1	本主机			
			127.0.0.0-127.255.255.255	
2	本地内网			
			10.0.0.0-10.255.255.255	
			172.16.0.0-172.31.255.255	
			192.168.0.0-192.168.255.255	
3	aa			

DCN | 神州数码 Digital China

➢ 系统状态

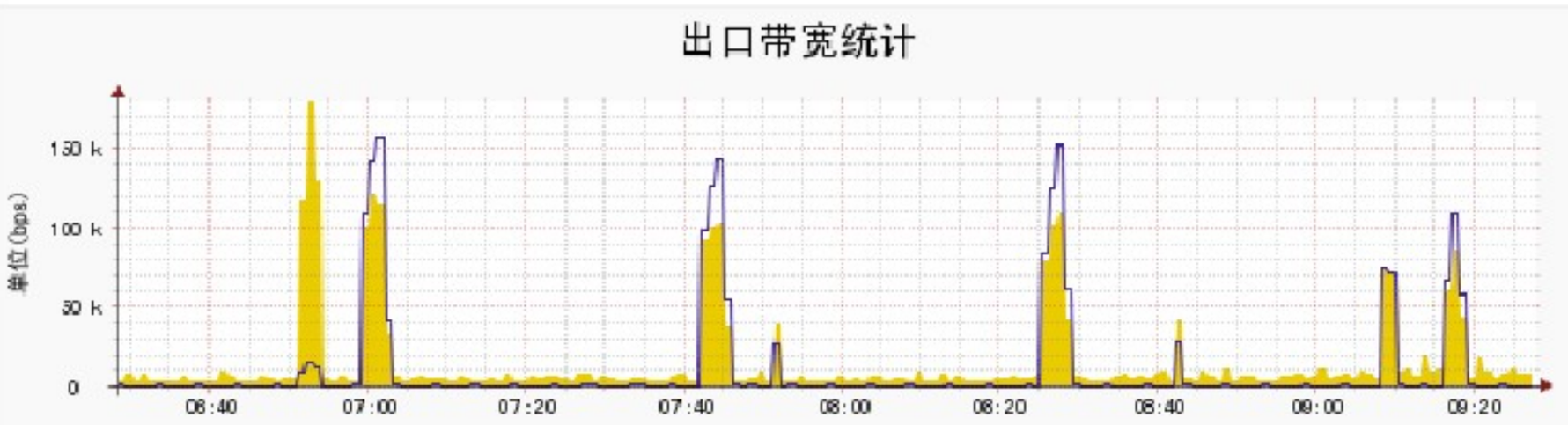
系统状态

开始时间：2011-02-11 06:2　　结束时间：2011-02-11 09:2

快捷查询：最近3小时　昨天　今天　最近7天　最近30天　查看

出口带宽统计

出口带宽统计



(2011-02-11 06:28:10 - 到 - 2011-02-11 09:28:10)

类型	——当前值——	——最大值——	——平均值——
下载:	7.01 k	178.99 k	14.59 k
上传:	7.87	156.47 k	10.17 k

最后更新时间：2011-02-11 09:27:35

状态监控

DCN | 神州数码 Digital China

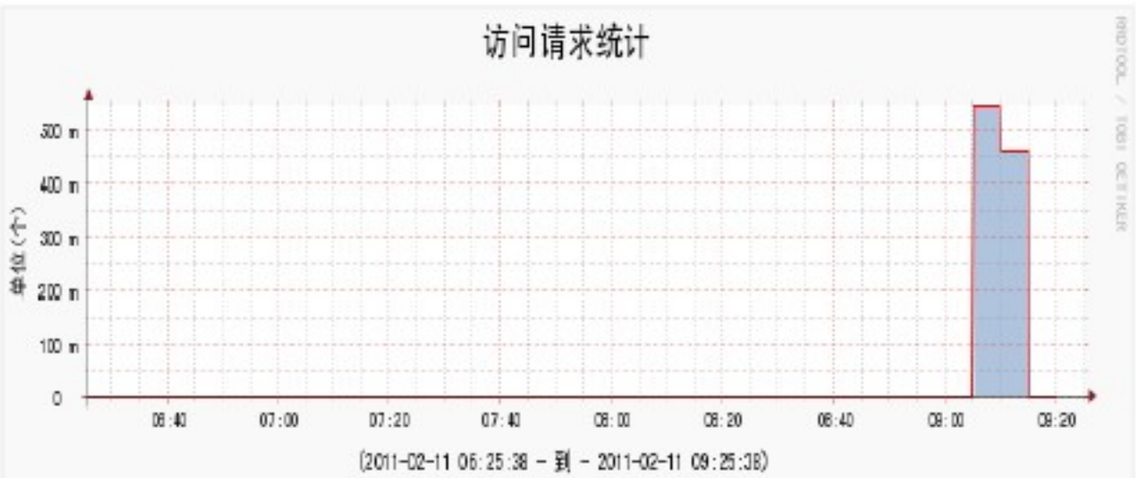
➢ 应用监控

应用状态(s191)

开始时间：2011-02-11 06:2　结束时间：2011-02-11 09:2

快捷查询：最近3小时　昨天　今天　最近7天　最近30天　查看

访问请求统计



类型	—当前值—	—最大值—	—平均值—
加速访问量:	0	0	0
未加速访问量:	0	1	0
总访问量:	0	1	0

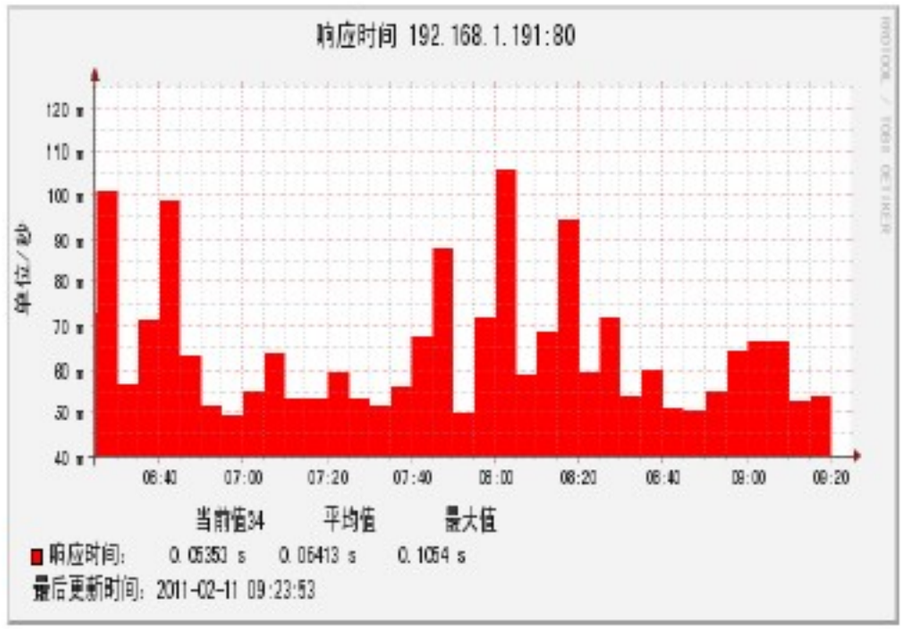
最后更新时间：2011-02-11 09:25:04

应用状态(s191)

开始时间：2011-02-11 06:24:27　结束时间：2011-02-11 09:24:27

快捷查询：最近3小时　昨天　今天　最近7天　最近30天　查看

主机 192.168.1.191:80



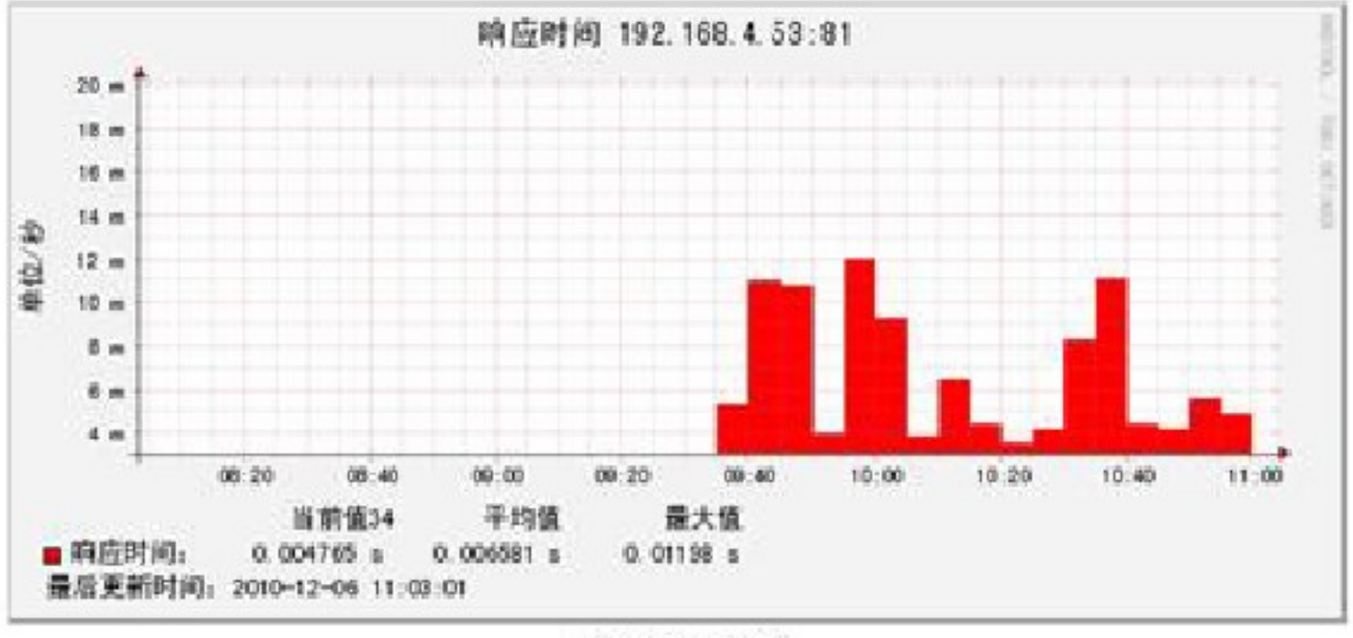
当前状态：正常

状态信息：HTTP OK: HTTP/1.1 200 OK - 8260 bytes in 0.064 second response time

状态监控

➢ 主机监控

主机 192.168.4.53:81



当前状态：正常

状态信息：HTTP OK: HTTP/1.1 200 OK - 14713 bytes in 0.005 second response time

日志报表

DCN | 神州数码 Digital China

- 日志：

可根据需要按不同的查询条件进行查询

基本攻击日志 | 爬虫防护日志 | CC防护日志 | 盗链防护日志 | 扫描防护日志 | 请求限制日志

基本攻击日志　　每页显示 10 条，当前第1/0页

服务：所有

方　法：所有　　源地址：

开始时间：　　结束时间：　　查询

时间	源地址	方法	URL地址	动作	策略	策略集	服务	白名单操作

站点访问日志

开始时间：　　结束时间：

客户端地址：　　方法：所有　　查询

序号	时间	客户端地址	地址来源	服务名称	访问URL	HTTP状态	响应时间
1	2011-02-11 09:09:47	192.168.1.206	局域网...	s191	http://192.168.1.191/	405	2
2	2010-12-07 17:40:33	192.168.2.14	局域网...	无	http://192.168.2.1:9090/a.php?user=45;%2...	404	4
3	2010-12-07 17:40:05	192.168.2.14	局域网...	无	http://192.168.2.1:9090/a.php?user=45;%2...	403	0

日志报表

- 报表

1、流量分析报表能直观的显示时段、每天、周、月的流量进行统计分析

2、访问者统计报表能对来自不同省市国家和地区的访问者进行统计

3、内容统计报表能对网站内容的访问次数及受众喜爱程度进行统计分析

4、攻击统计报表能根据需求对不同时段和来源的攻击进行统计分析，以使管理者能够根据统计数据制定不同的访问和防护策略

系统维护

➢ 用户管理

系统中的管理用户分为三类：系统管理员、审计管理员、配置管理员，分别具有不同权限。

用户管理

新建...

序号	用户名	用户类型	电子邮件	修改	删除
1	admin	系统管理员			
2	a	审计管理员			
3	b	配置管理员			

系统维护

➢ 系统升级

系统信息

引擎升级

引擎升级包： 浏览... 升级

版本信息： *当前版本没有进行过此部分的升级/更新。*

升级提示： 升级完成后需要重启网关。

授权证书导入

授权证书： 浏览... 导入

硬件特征码： F158-839E-A2CE-DAD0

—网络创造价值—

系统诊断

网络工具测试

*工具： PING测试 *主机： 192.168.1.254 *时长： 4 网口： tiger 执行

```
PING 192.168.1.254 (192.168.1.254) from 192.168.1.195 tiger: 56(84) bytes of data.
64 bytes from 192.168.1.254: icmp_seq=1 ttl=64 time=0.776 ms
64 bytes from 192.168.1.254: icmp_seq=2 ttl=64 time=0.973 ms
64 bytes from 192.168.1.254: icmp_seq=3 ttl=64 time=1.71 ms
64 bytes from 192.168.1.254: icmp_seq=4 ttl=64 time=1.43 ms
--- 192.168.1.254 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3015ms
rtt min/avg/max/mdev = 0.776/1.223/1.710/0.370 ms
```

网络信息查看

查看ARP表 查看主路由表 查看管理口策略路由 查看网卡信息

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.6.0     0.0.0.0         255.255.255.0   U     0      0        0 管理口
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 WAN
192.168.45.0    0.0.0.0         255.255.255.0   U     0      0        0 带外口
169.254.0.0     0.0.0.0         255.255.0.0     U     0      0        0 管理口
0.0.0.0         192.168.1.254   0.0.0.0         UG    0      0        0 WAN
```

其他配置

DCN | 神州数码 Digital China

➢ 时间配置

➢ HA配置

双机热备配置

配置参数

工作模式：	◉主设备 ○从设备
心跳口标识：	mng
本地心跳地址：	223.23.23.3/255.255.255.0
对端心跳地址：	192.168.4.46
	保存

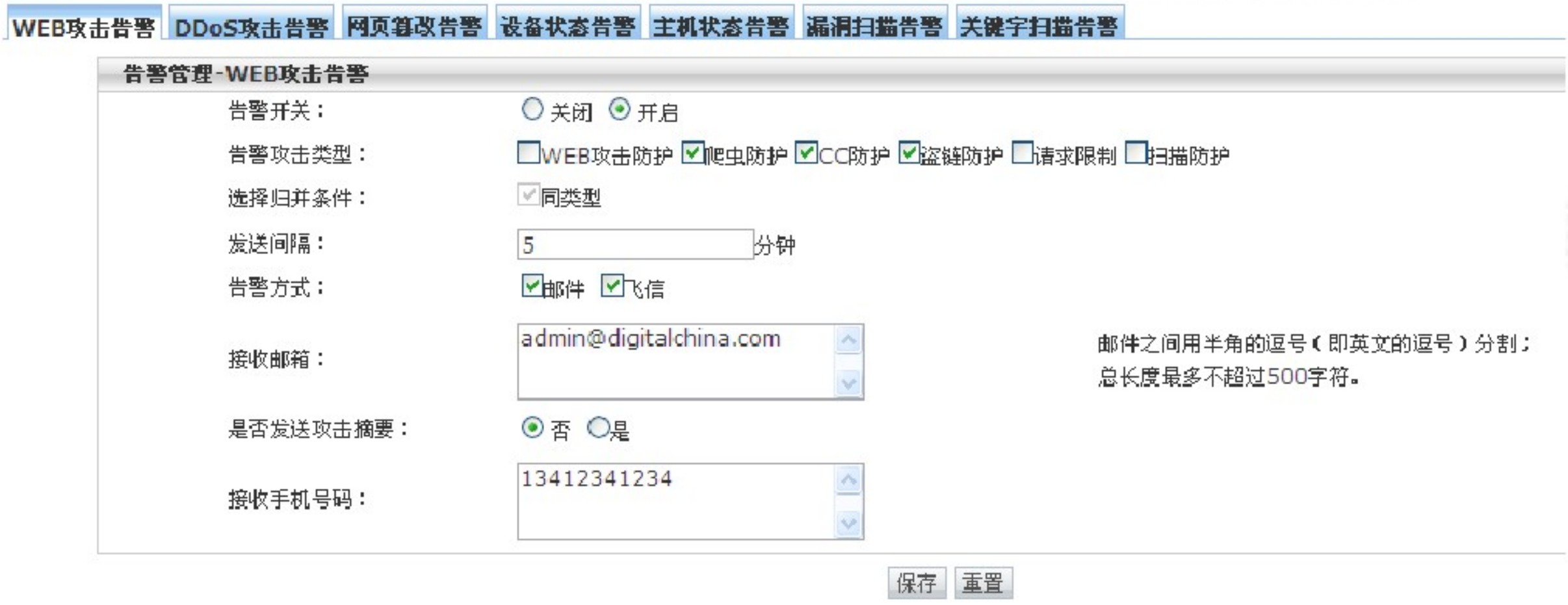
状态切换

当前状态：	已关闭

其他配置

➢ 告警配置

告警配置首先要进行邮件服务器的配置，才可以进行邮件告警，邮件服务器配置类似于**foxmail**



DCN | 神州数码 Digital China

➢ 日志配置

日志归档 | 自动导出 | 手动导出 | 日志清空 | 日志功能管理

自动导出

日志类型：
- [ ] WEB防护日志
- [x] DDoS防护日志
- [x] 篡改日志
- [x] 操作日志
- [ ] 防篡改镜像日志
- [ ] 防篡改重定向日志

导出时间： 每天 | 请选择日期

FTP主机： 192.168.2.48

FTP端口： 21

FTP登录用户名： asasd

FTP登录密码： •••••

FTP上传路径： /

确定 | 重置 | 关闭自动导出

常见故障排除

- 查询不到访问日志？
  - 选择的查询日期是否正确？
  - 日志配置中是否打开记录日志的开关？
  - 该服务是否选择记录访问日志？
- 没有收到告警邮件？
  - 是否配置攻击告警？
  - 邮件发送配置是否正确配置？
  - 网络是否正常？
  - DNS是否正确？
- 切换直通后，管理口无法访问WEB管理界面？
  - 使用带外口登录系统
  - 确认直通前管理口是否正确配置IP地址？
  - 确认是否配置管理口策略路由？

DCN

网 络 创 造 价 值

谢谢！

我们的理想就在于，通过把握领先的网络发展技术趋势，采取形式多样的技术合作，结合我们对国内客户的充分理解，以及坚持以应用为导向的研发和服务体系，构造出一个满足用户需求的智能化网络，因此我们就提出了让网络应用普遍成功的理念。

让网络应用普遍成功

欲了解更多详情，请访问
www.dcnetworks.com.cn