



WAN

1.

2. URL

URL

URL IDP

URL IDP

URL IDP

URL

URL

URL

URL

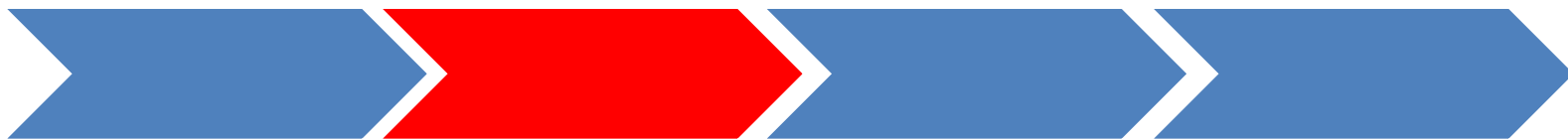
```

>
/24
>
WAN
eth1 eth0
IP
10.2.4.5/21
LAN WAN eth0 LAN eth1

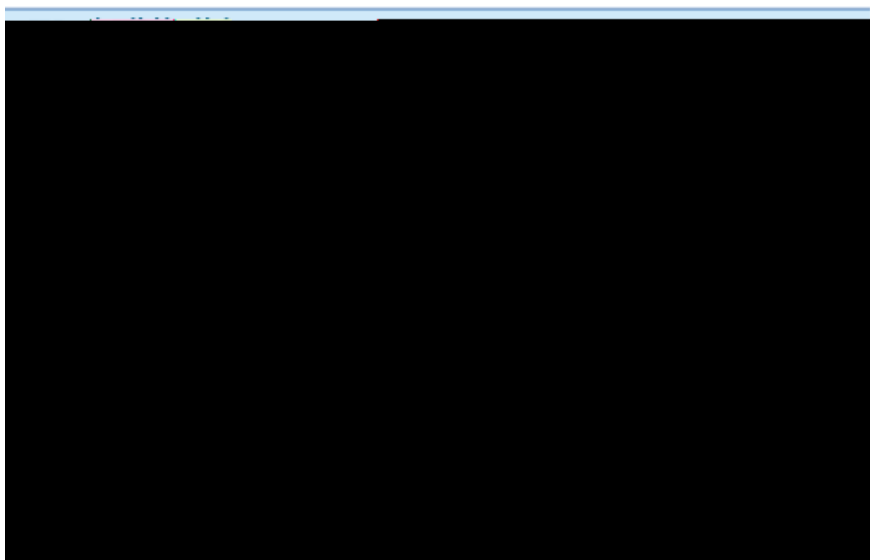
```

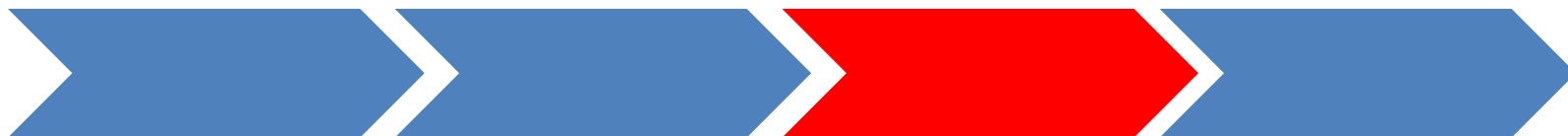


profile1



apppolicy1





URL

URL

URL

URL

URL

1. URL Whitelist1,
www.google.com.hk

URL www.sina.com.cn

2. Blacklist1,
www.aol.com

URL www.msn.com

◆ IPS ◆ 出口控制 ◆ URL过滤 ◆ 黑白名单

名称 *

描述

类型

URL列表 (总数: 2)

URL	描述
www.sina.com.cn	
www.google.com.hk	

◆ IPS ◆ 出口控制 ◆ URL过滤 ◆ 黑白名单

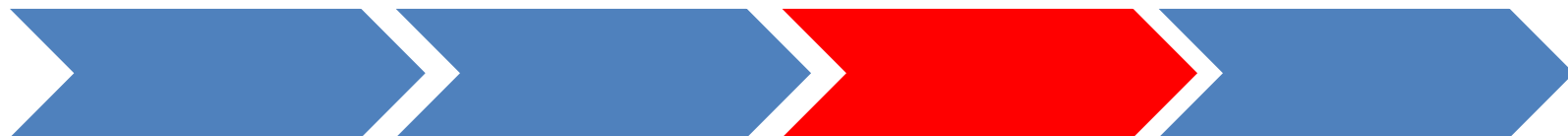
名称 *

描述

类型

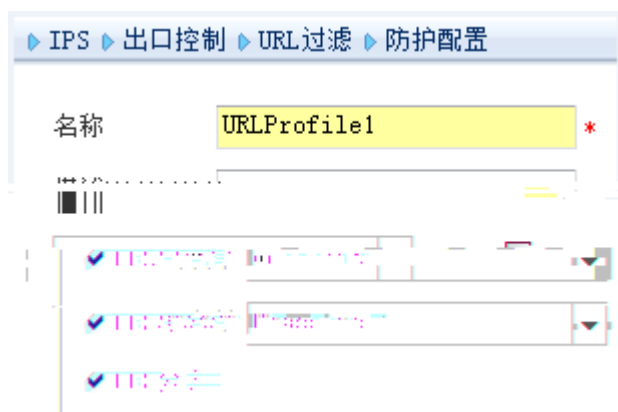
URL列表 (总数: 2)

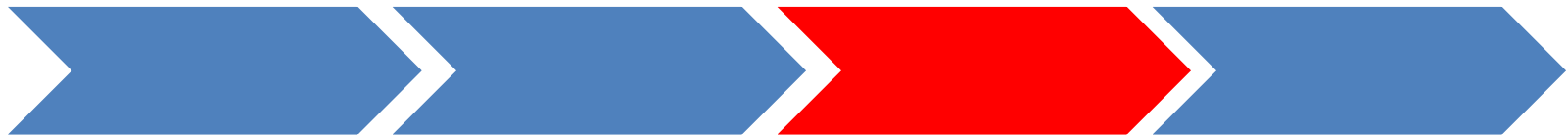
URL	描述	启用
www.msn.com		✓
www.aol.com		✓



URL

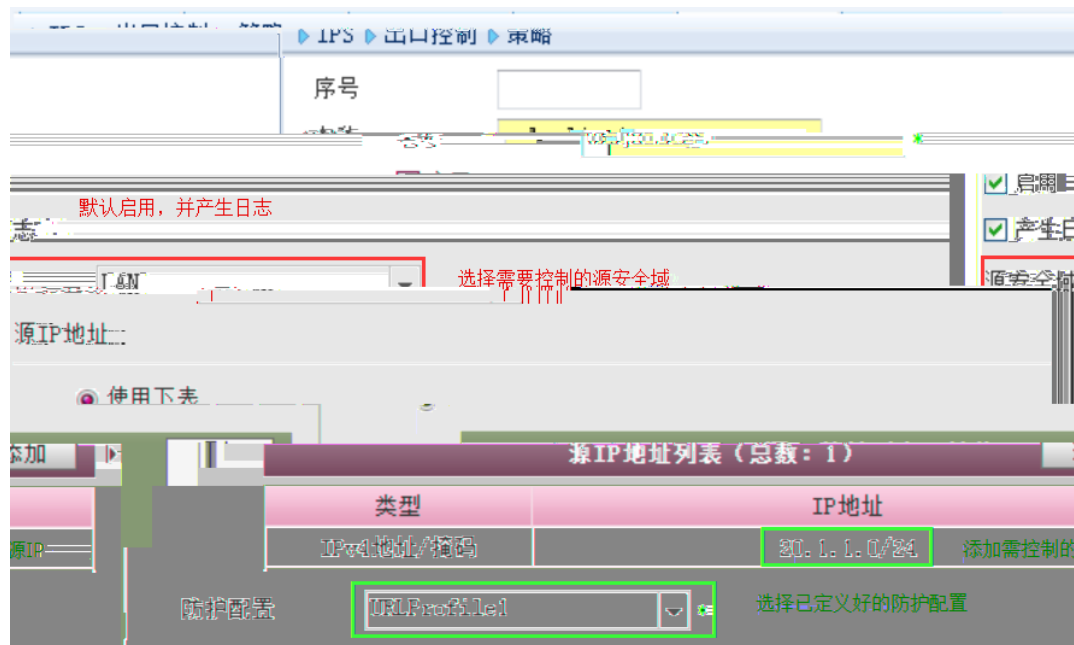
URL





URL

1. WAN URL
2. URL URL urlpolicy1





1. Google-Talk Skype

2. Google-Talk Skype

URL

1. www.google.com.hk www.sina.com.cn

2. www.msn.com www.aol.com URL

3. URL

4. URL

URL



ï € ... F å

Ø ¢ u

Ô ‘ y f u

î , [Ä à ï € * IDP ; û à g * ’ k 4 + ï € ¶ g ... k ’
ò t U Y F å , • ï € ... k o x à Ž d y g IPShož



WAN

◆ IPS ◆ 客户端防护 ◆ 策略

安全域 *

☒ 开 保护此安全域的客户端



clientpolicy1

IP

IPS

IPS 安全策略配置

名称: clientpolicy1

☒ 启用

☒ 产生日志

客户端IP地址

☐ 任意

☐ 任意IPv4地址

☐ 任意IPv6地址

使用下表

类型	IP地址
地址/掩码	20.1.1.0/24

客户端IP地址 (总数: 1) 添加

中

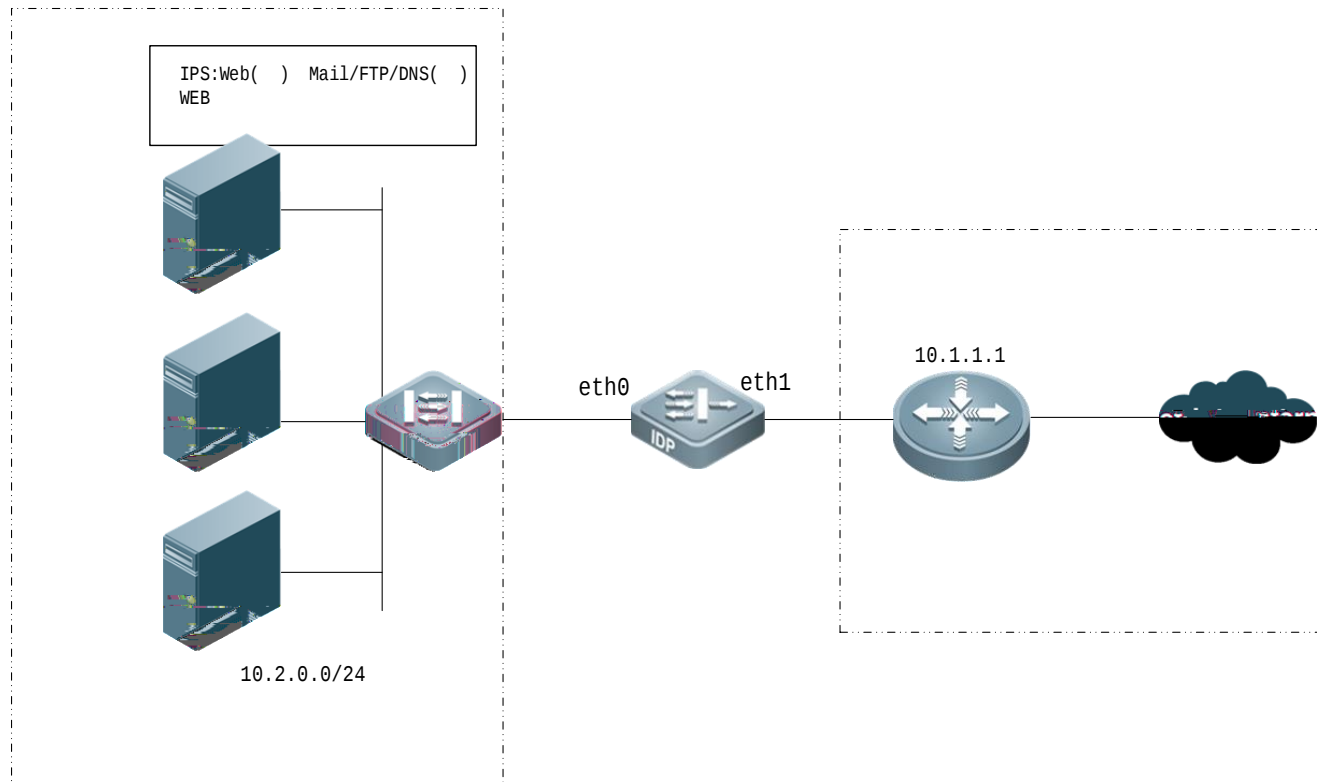
低 中 高 自定义 Client_Media

IPS

关闭

clientpolicy1





IDP LAN Web FTP DNS

LAN DMZ

1.

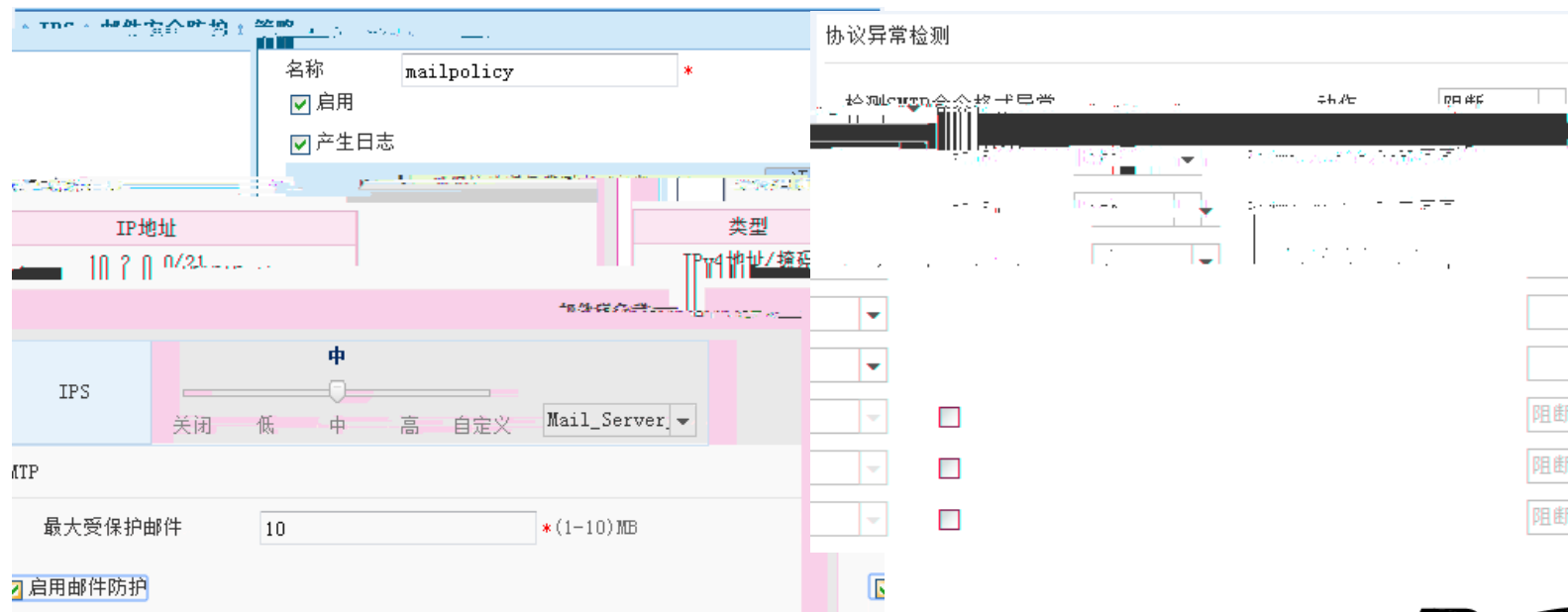


1.

安全域 *

☒ 开 保护此安全域的客户端

2.





1.

FTP

2.

► IPS ► FTP安全防护

名称 *

☒ 启用

☒ 产生日志

受保护的服务器列表 (总数: 1) ►

类型	IP地址
IPv4地址/掩码	10.2.0.0/21

FTP服务器

IPS

关闭 低 中 高 自定义 ▼

1.



1. **IPS>** >
- 2.
- 3.

IPS > 邮件安全防护 > 邮件防护

信息泄露防护

☒ 产生日志

☒ 将SMTP服务器标题信息替换为 (0-256)

☒ 将POP3服务器标题信息替换为 (0-256)

☒ 将IMAP服务器标题信息替换为 (0-256)



1. DoS
- 2.
3. TCP
4. IP
5. ICMP

TCP SYN cookie

IP tcp syn

攻击防御 > 攻击防御 > DoS防御

将下列设置应用于安全域 wan

☒ ICMP泛滥	阈值 10000 *pps	☒ 报警 ☒ 丢弃
☒ TCP SYN泛滥	阈值 100000 *pps	☒ 报警 ☒ 丢弃
☒ UDP泛滥	阈值 100000 *pps	☒ 报警 ☒ 丢弃
☒ DNS泛滥	阈值 100000 *pps	☒ 报警 ☒ 丢弃
☐ TCP RST扫描		☐ 报警 ☐ 丢弃
☒ 报警 ☒ 丢弃 ☒ 报警 ☒ 丢弃 ☒ 丢弃 ☒ 丢弃		
☒ LAND ☒ Smurf ☒ Ping of Death ☒ Teardrop ☐ TCP SYN Cookie		

确定 取消

攻击防御 > 攻击防御 > 探测防御

将下列设置应用于安全域

wan

攻击防御设置

速率 1000 字节

攻击防御设置

☒ TCP SYN端口扫描

阈值 1 *秒

☒ 报警 ☒ 丢弃

☒ TCP FIN扫描

☒ 报警 ☒ 丢弃

☒ TCP XMAS扫描

☒ 报警 ☒ 丢弃

☒ TCP NULL扫描

☒ 报警 ☒ 丢弃

☐ 设置TCP SYN和FIN标志

☐ 丢弃

☐ 无ACK标志的TCP FIN标志

☐ 丢弃

☐ 非SYN标志

☐ 丢弃

确定

取消

TCP

攻击防御

攻击防御

TCP逃避控制

2

将下列设置应用于安全域

wan

TCP逃避控制

*每条连接中的RST包

最多允许

5

☒ 报警

☒ 丢弃

☒ Small PMTU

最小MTU

350

*字节

☒ 丢弃

☒ TCP控制位异常

☒ 丢弃

☒ TCP数据重叠

TCP保护

☒ 校验ICP序列号

探测不符合连接状态的

所有

数据包

确定

取消

IP

攻击防御

攻击防御

TCP逃避控制

2

将下列设置应用于安全域

wan

TCP逃避控制

*每条连接中的RST包

最多允许

5

☒ 报警

☒ 丢弃

☐ 丢弃

☐ 丢弃

☒ Small PMTU

最小MTU

350

*字节

☒ TCP控制位异常

☒ TCP数据重叠

TCP保护

☒ 校验TCP序列号

探测不符合连接状态的

所有

数据包

确定

取消

34 | www.ruijie.com.cn

| www.ruijie.com.cn

Ruijie

ICMP

▲ 攻击防御 ▲ 攻击防御 ▲ ICMP 攻击防御

将下列设置应用于安全域 wan

☒ 报警 ☒ 丢弃

☒ ICMP_SSS_Pinger

Ping	☒ 报警 ☒ 丢弃	☐ ICMP L3retriever
Echo	☒ 报警 ☒ 丢弃	☐ ICMP Nemesis v1.1
	☒ 报警 ☒ 丢弃	☐ ICMP Ping NMAP
1.1	☒ 报警 ☒ 丢弃	☐ ICMP Icmpenum v1.
t	☒ 报警 ☒ 丢弃	☒ ICMP Redirect Hos
	☒ 报警 ☒ 丢弃	☒ ICMP Redirect Net
ho	☒ 报警 ☒ 丢弃	☐ ICMP Superscan Ec
POPTs	☒ 报警 ☒ 丢弃	☐ ICMP Traceroute I
anner	☒ 报警 ☒ 丢弃	☐ ICMP Webtrends Sc
	☐ ICMP Source Quench	☒ 报警 ☒ 丢弃
	☐ ICMP Broadscan Smurf Scanner	☒ 报警 ☒ 丢弃
	☒ 报警 ☒ 丢弃	☐ ICMP Ping Speedera
	☒ 报警 ☒ 丢弃	☐ ICMP TJPingPro1.1Build 2 Windows
	☒ 报警 ☒ 丢弃	☐ ICMP Ping Whatsup Gold Windows
	☒ 报警 ☒ 丢弃	☐ ICMP Ping CyberKit2.2 Windows

- www.huawei.com.cn

- www.huawei.com.cn/service.aspx

- support.huawei.com.cn

- webchat.huawei.com.cn

- 4008-111-000