

LAN

URL

IDP

WAN

1.

2. URL

URL

URL IDP

URL IDP

URL IDP

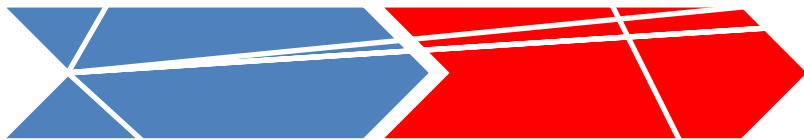
URL

URL

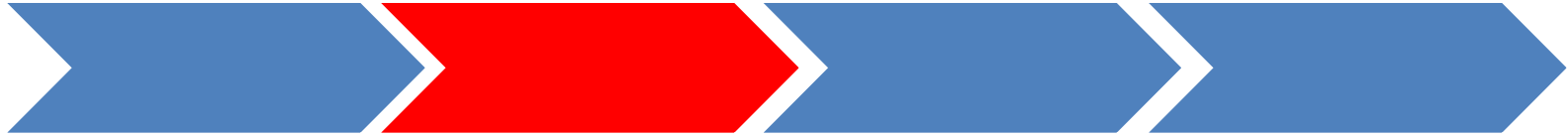
URL

URL

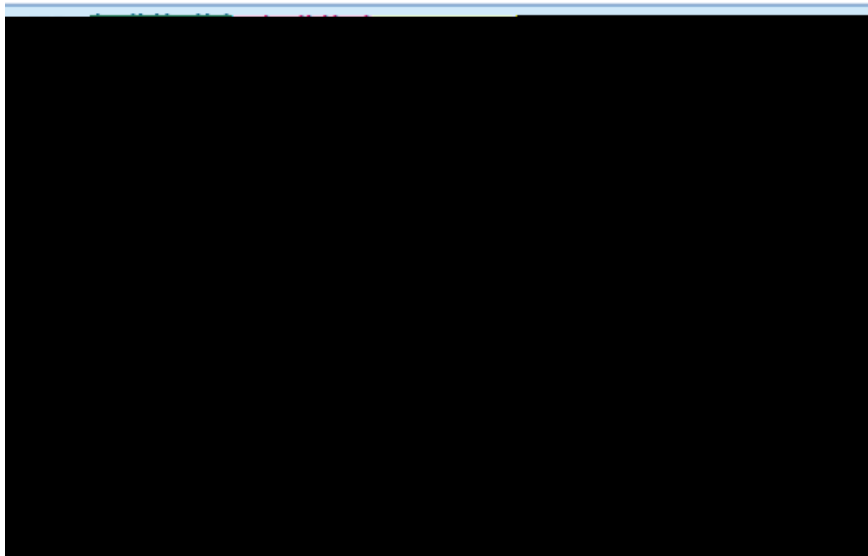
1. > eth1 eth0 IP 10.2.4.5/24
20.1.1.1/24
2. > LAN WAN eth0 LAN eth1
WAN
- 3.

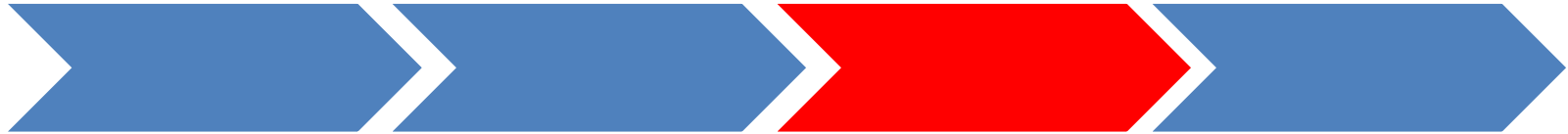


profile1



apppolicy1





URL

URL

URL

URL

URL

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

2. Blacklist1, URL www.msn.com
www.aol.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

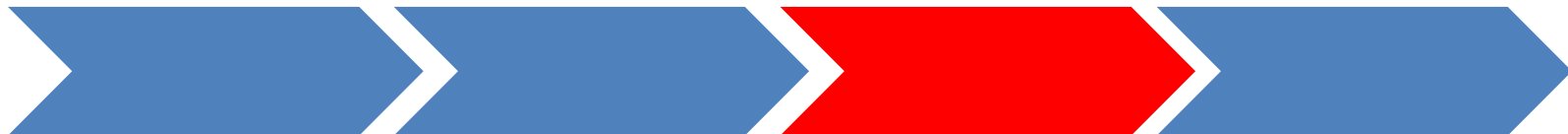
名称 *

描述

类型

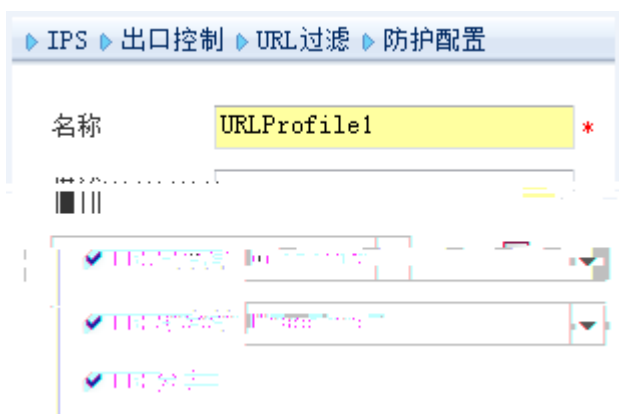
URL列表 (总数: 2)

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



URL

URL



名称	启用	动作	分类	备注	
标题广告和弹出式广告)的	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	广告	提供广告图片或其他广告内容文件(如
服务的网站。	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	烟酒	推销烟酒相关产品或服



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 ç 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





clientpolicy1

IP

IPS

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

IP地址
20.1.1.0/24

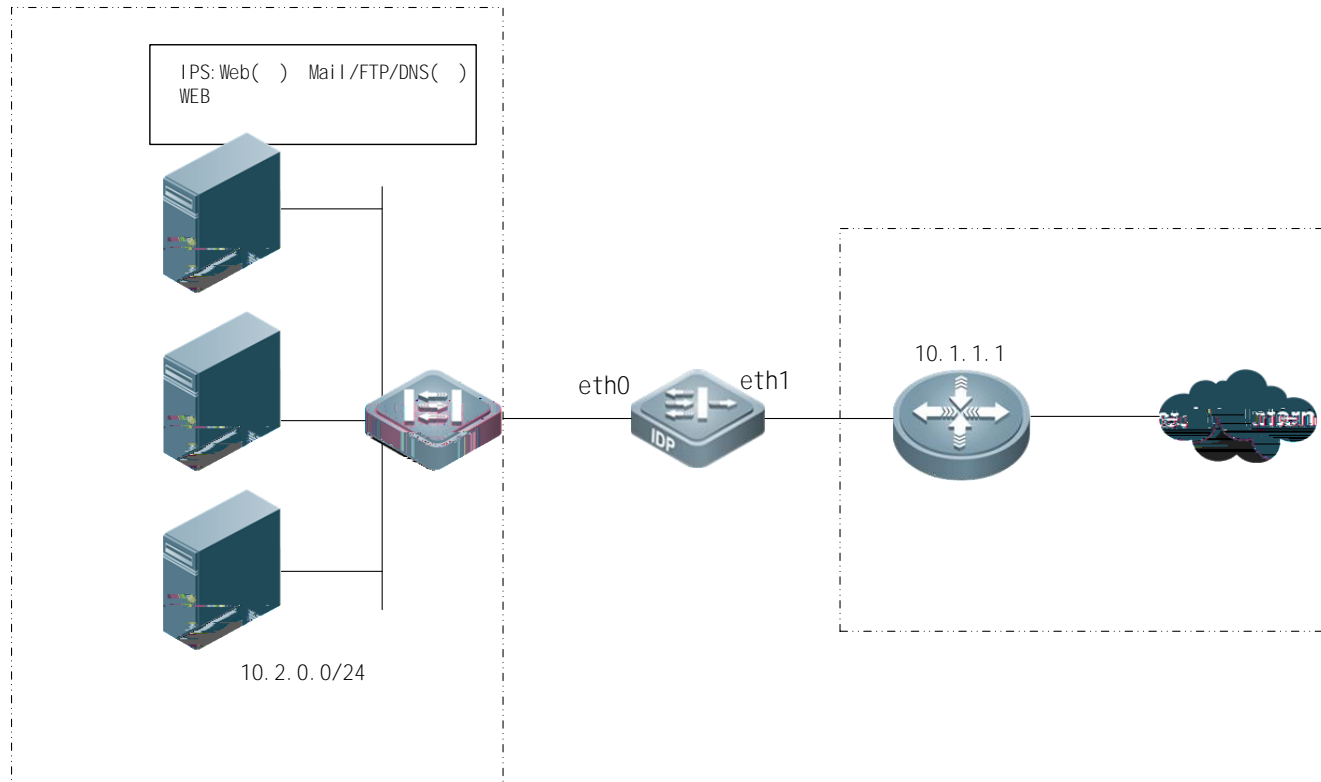
中

中 高 自定义 Client_Media

IPS 关闭 低

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.

The screenshot shows the configuration page for a mail policy named "mailpolicy". The "名称" (Name) field is "mailpolicy" with a red asterisk. The "启用" (Enable) and "产生日志" (Generate Log) checkboxes are checked. The "协议异常检测" (Protocol Anomaly Detection) section is visible, showing a table with columns for "名称" (Name), "IP地址" (IP Address), "类型" (Type), and "动作" (Action). The "动作" column contains "阻断" (Block) for three entries. The "IPS" section shows a slider set to "中" (Medium) and a dropdown menu set to "Mail_Server". The "最大受保护邮件" (Maximum Protected Mail) field is set to "10" MB. The "启用邮件防护" (Enable Mail Protection) checkbox is checked.



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

<input checked="" type="checkbox"/> 产生日志		
<input checked="" type="checkbox"/> 将SMTP服务器标题信息替换为	<input type="text" value="Mail Server Ready..."/>	(0-256)
<input checked="" type="checkbox"/> 将POP3服务器标题信息替换为	<input type="text" value="Mail Server Ready..."/>	(0-256)
<input checked="" type="checkbox"/> 将IMAP服务器标题信息替换为	<input type="text" value="Mail Server Ready..."/>	(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

<input checked="" type="checkbox"/> ICMP泛滥	阈值 <input type="text" value="10000"/> *pps	<input checked="" type="checkbox"/> 报警 <input checked="" type="checkbox"/> 丢弃
<input checked="" type="checkbox"/> TCP SYN泛滥	阈值 <input type="text" value="100000"/> *pps	<input checked="" type="checkbox"/> 报警 <input checked="" type="checkbox"/> 丢弃
<input checked="" type="checkbox"/> UDP泛滥	阈值 <input type="text" value="100000"/> *pps	<input checked="" type="checkbox"/> 报警 <input checked="" type="checkbox"/> 丢弃
<input checked="" type="checkbox"/> DNS泛滥	阈值 <input type="text" value="100000"/> *pps	<input checked="" type="checkbox"/> 报警 <input checked="" type="checkbox"/> 丢弃
<input type="checkbox"/> TCP RST扫描		<input type="checkbox"/> 报警 <input type="checkbox"/> 丢弃

报警 丢弃

报警 丢弃

丢弃

丢弃

LAND

Smurf

Ping of Death

Teardrop

ICP 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

扫描探测防御

TCP SYN端口扫描

TCP FIN扫描

TCP XMAS扫描

TCP NULL扫描

设置TCP SYN和FIN标志

无ACK标志的TCP FIN标志

非SYN标志

速率 3000 字节

阈值 1 *秒

报警/丢弃/日志

报警 丢弃

报警 丢弃

报警 丢弃

报警 丢弃

丢弃

丢弃

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

TCP逃避控制

启用 禁用 策略 策略

*每条连接中的RST包 最多允许

PMTU *字节 报警 丢弃 Small

削位异常 丢弃 TCP控制

源重叠 丢弃 TCP数封

TCP保护

TCP校验和 报警 丢弃 校验TC

TCP序列号 探测不符合连接状态的 数据包 报警 丢弃 校验TC

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

TCP逃避控制

启用 禁用 策略 策略

*每条连接中的RST包

最多允许

PMTU 最小MTU *字节 报警 丢弃

削位异常 丢弃

源重叠 丢弃

IP校验和 探测具有非法校验和的数据包 报警 丢弃

IP序列号 探测不符合连接状态的 数据包 报警 丢弃

TCP保护

Small

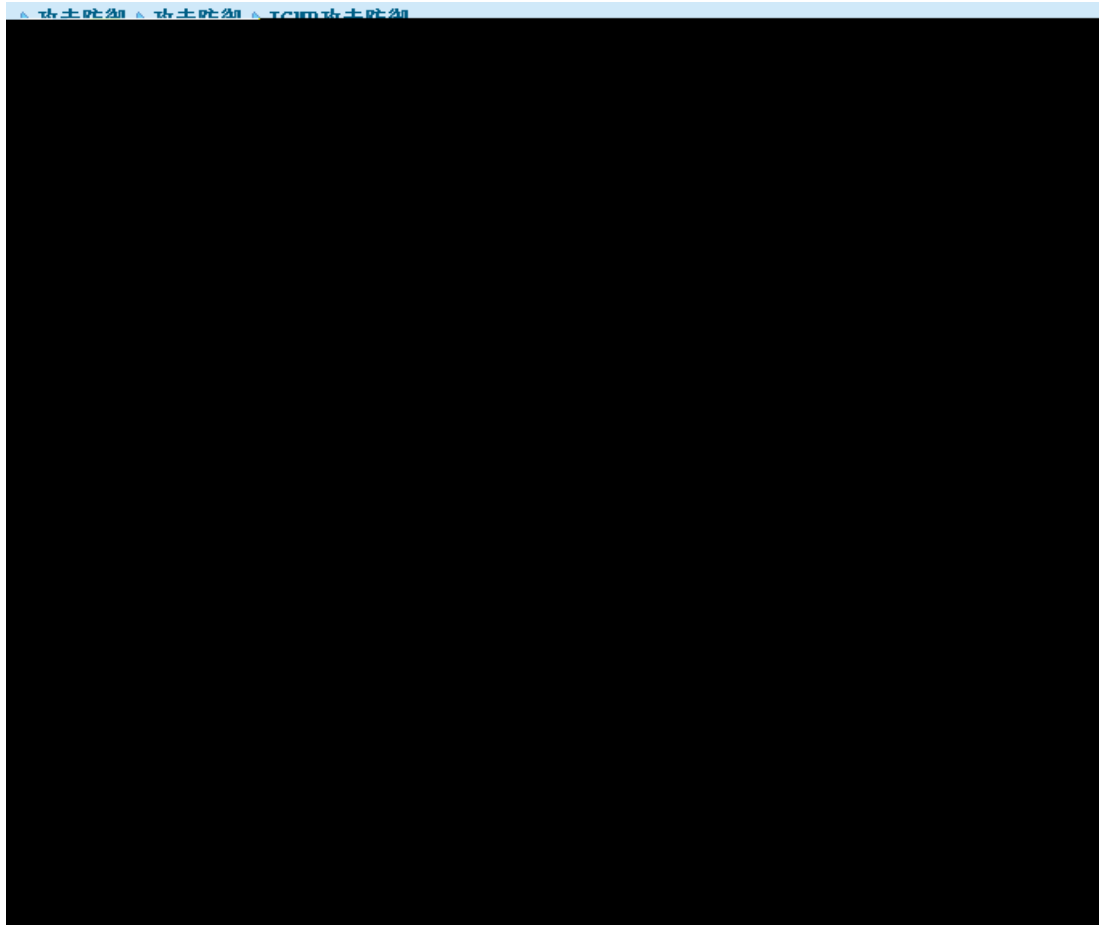
TCP控制

TCP数据

校验TC

校验TC

ICMP



- www.ruijie.com.cn

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

- support.ruijie.com.cn

- webchat.ruijie.com.cn

- 4008-111-000