

WA1208E的防火墙功能配置实例

适用WA1208E版本: E1101版本

适用WA1208E型号: WA1208E-G / WA1208E-DG / WA1208E-AG / WA1208E-AGP

一、组网需求

对组网无特殊需求。

二、配置步骤

防火墙配置任务的要求如下:

- MAC地址为00e0-fc00-0001的用户不能接入AP, 其余的可以接入。
- 源MAC地址为00aa-00aa-00aa的用户报文不能发送到AP的无线侧。
- 源IP地址为192.168.0.0/24 网段的报文不能由无线侧进入AP。
- ICMP报文不能发送到AP的无线侧。

1、定义ACL规则。

```
[H3C]acl 200
[H3C-acl-mac-200]rule 0 deny source-mac 00e0-fc00-0001
[H3C-acl-mac-200]quit
[H3C]acl 700
[H3C-acl-advmac-700]rule 0 deny source-mac 00aa-00aa-00aa
[H3C-acl-advmac-700]quit
[H3C]acl 2000
[H3C-acl-basic-2000]rule 0 deny source 192.168.0.0 0.0.0.255
[H3C-acl-basic-2000]quit
[H3C]acl 3000
[H3C-acl-adv-3000]rule 0 deny icmp
[H3C-acl-adv-3000]quit
[H3C]ssid Huawei
New ssid!
```

2、开启黑白名单的防火墙, 并且应用ACL 200规则, 实现“MAC地址为00e0-fc00-0001的用户不能接入AP, 其余的可以接入”。

```
[H3C-ssid-Huawei]firewall access enable
[H3C-ssid-Huawei]firewall access default permit
[H3C-ssid-Huawei]firewall access 200
ACL applied successfully
```

3、开启包过滤的防火墙, 在out方向应用ACL 700规则, 实现“源MAC地址为00aa-00aa-00aa的用户报文不能发送到AP的无线侧”。

```
[H3C-ssid-Huawei]firewall packet enable
[H3C-ssid-Huawei]firewall packet default permit
[H3C-ssid-Huawei]firewall packet 700 outbound
ACL applied successfully
```

4、在in方向应用ACL 2000, 实现“源IP地址为192.168.0.0/24 网段的报文不能由无线侧进入AP”。

```
[H3C-ssid-Huawei]firewall packet 2000 inbound
ACL applied successfully
```

5、在out方向应用ACL 3000, 实现“ICMP报文不能发送到AP的无线侧”。

```
[H3C-ssid-Huawei]firewall packet 3000 outbound
ACL applied successfully
```

6、查看防火墙信息。

```
[H3C-ssid-Huawei]display firewall packet-filter statistics ssid Huawei
SSID: Huawei
Firewall enabled
Firewall's default filtering method set to 'permit'
In-bound Policy: acl 700
In-bound Policy: acl 2000
From 2002-01-02 05:56:52 to 2002-01-02 06:27:39
  0 packets, 0 bytes, 0% permitted,
  0 packets, 0 bytes, 0% denied,
  0 packets, 0 bytes, 0% permitted default,
  0 packets, 0 bytes, 0% denied default,
Totally 0 packets, 0 bytes, 0% permitted,
```

Totally 0 packets, 0 bytes, 0% denied.

Out-bound Policy: acl 3000

From 2002-01-02 05:56:45 to 2002-01-02 06:27:41

0 packets, 0 bytes, 0% permitted,

0 packets, 0 bytes, 0% denied,

0 packets, 0 bytes, 0% permitted default,

0 packets, 0 bytes, 0% denied default,

Totally 0 packets, 0 bytes, 0% permitted,

Totally 0 packets, 0 bytes, 0% denied

7、查看黑白名单统计信息

[H3C-ssid-Huawei]display firewall access statistics ssid Huawei

SSID Huawei

Firewall enabled

Firewall's default filtering method set to 'permit'

acl 200

From 2002-01-02 06:11:33 to 2002-01-02 06:29:25

0 users, 0% permitted,

0 users, 0% denied,

0 users, 0% permitted default,

0 users, 0% denied default,

Totally 0 users, 0% permitted,

Totally 0 users, 0% denied.