修订记录

本页不打印

课程编码	适用产品	产品版本	课程版本

作者/工号	时间	审核人/工号	新开发/优化
万倡利/wwx408647	2020.03.11		

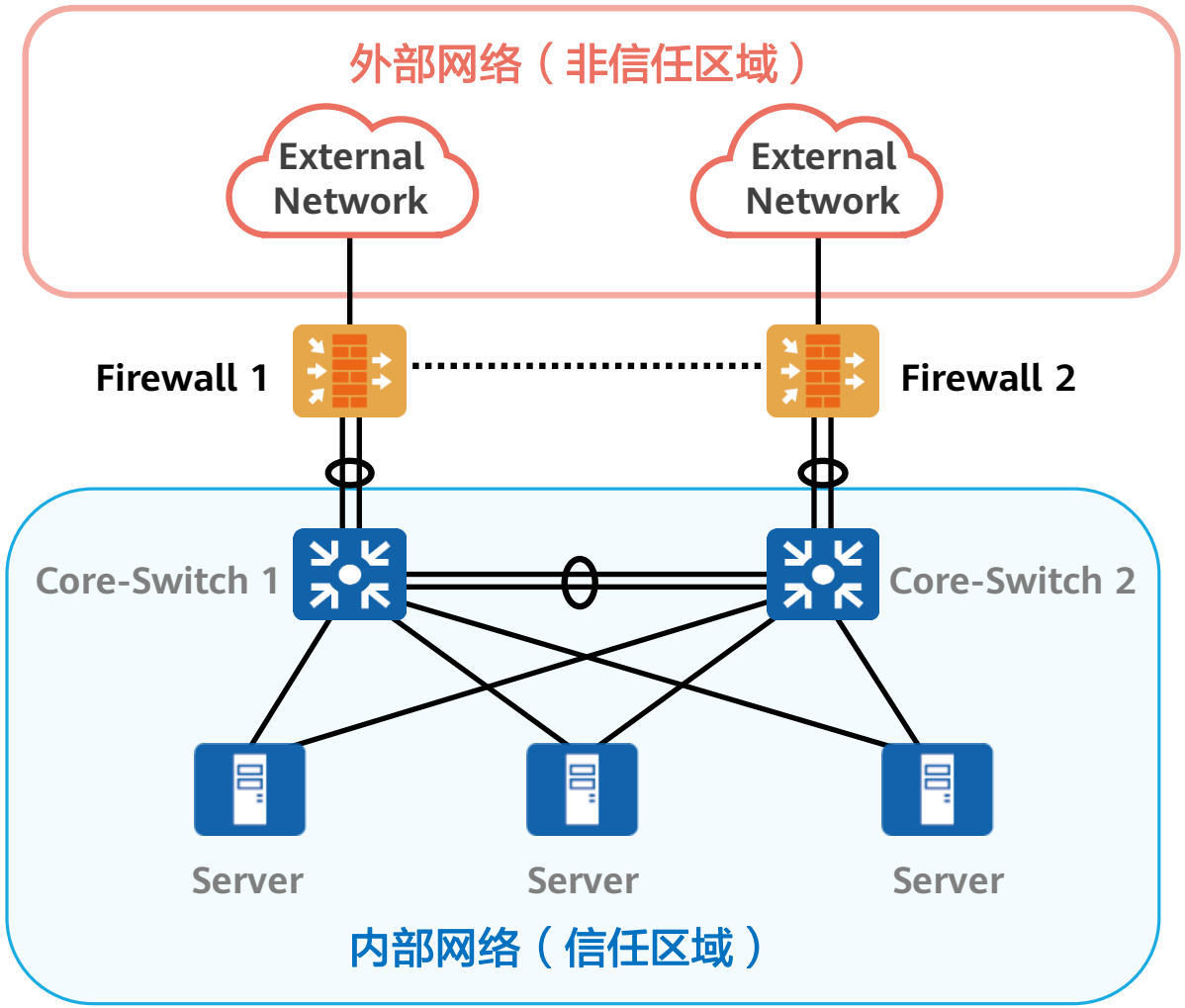
网络安全威胁与防御

目标

- 学完本课程，您将能够：
  - 阐明防火墙的基本概念，例如安全区域、安全策略、会话表等
  - 实现防火墙的基本配置
  - 描述DDoS攻击
  - 配置网络反病毒技术
  - 配置用户管理

目录

为什么需要防火墙?



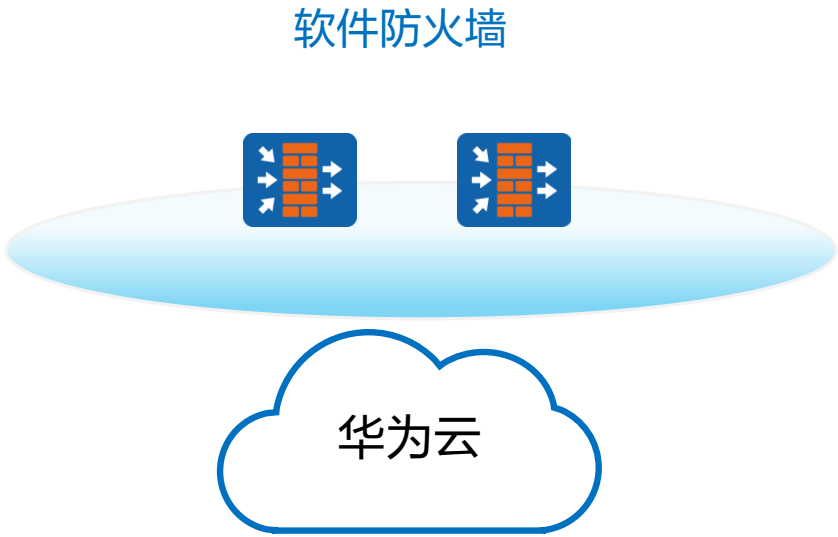
- 安全无处不在。路由器和交换机构建了互联互通的网络，带来便利的同时也带来了安全隐患。
- 例如在网络边界，企业有了如下安全诉求：
  - 外部网络安全隔离
  - 内部网络安全管控
  - 内容安全过滤
  - 入侵防御
  - 反病毒

什么是防火墙?

- 在通信领域，防火墙是一种安全设备。它用于保护一个网络区域免受来自另一个网络区域的攻击和入侵，通常被应用于网络边界，例如企业互联网出口、企业内部业务边界、数据中心边界等。
- 防火墙根据设备形态分为，框式防火墙、盒式防火墙和软件防火墙，支持在云上云下灵活部署。

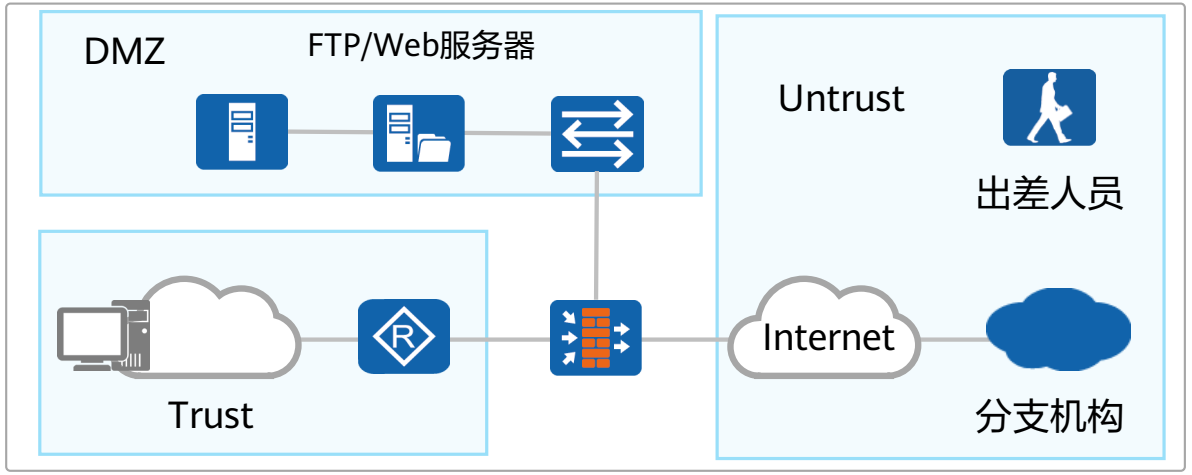
框式防火墙

盒式防火墙

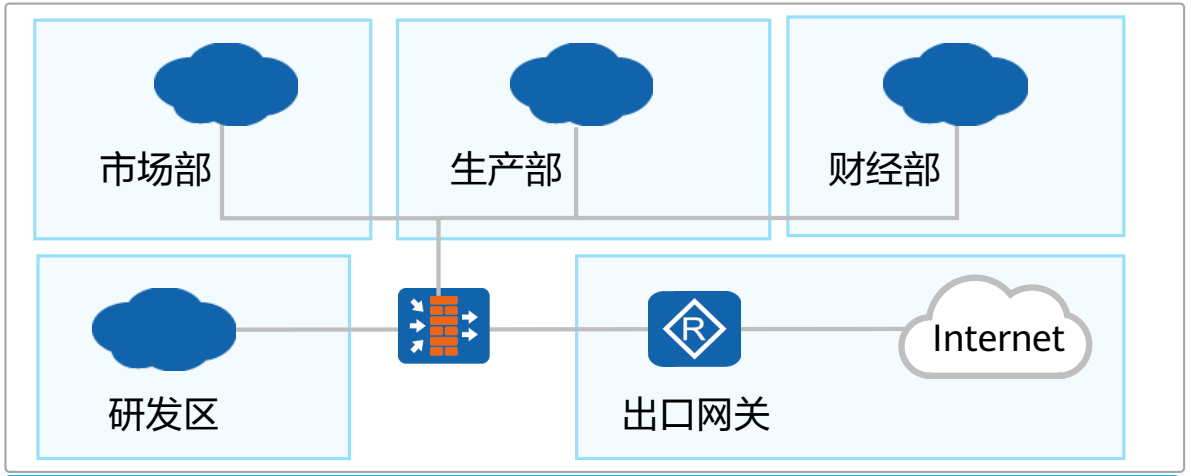


防火墙的典型应用场景

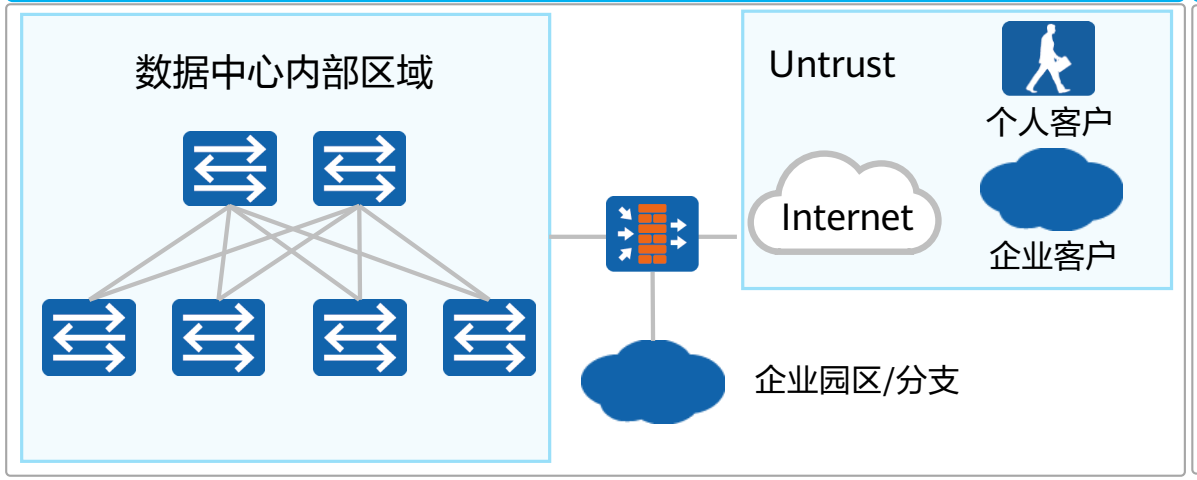
企业边界防护



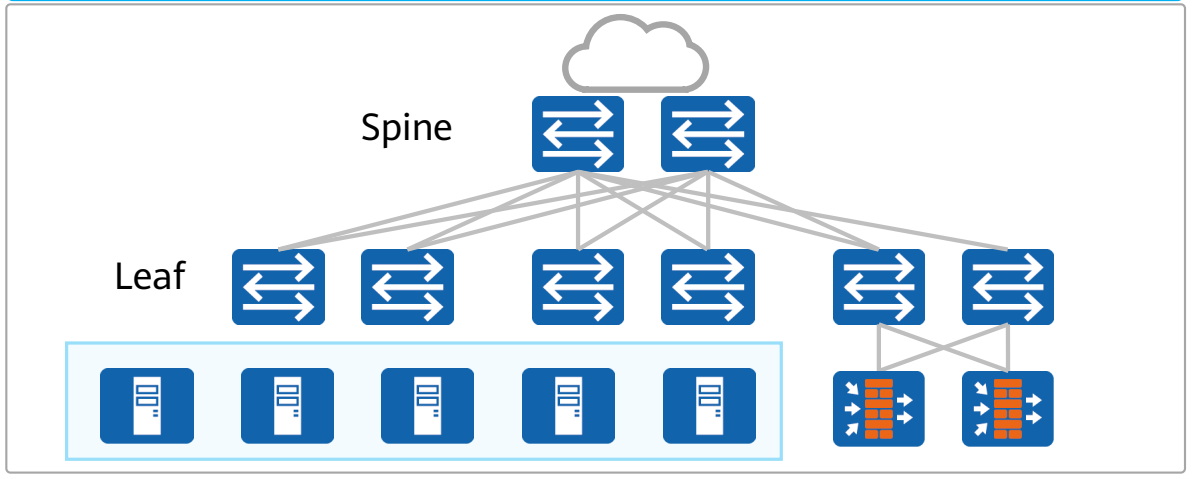
内网管控与安全隔离



数据中心边界防护

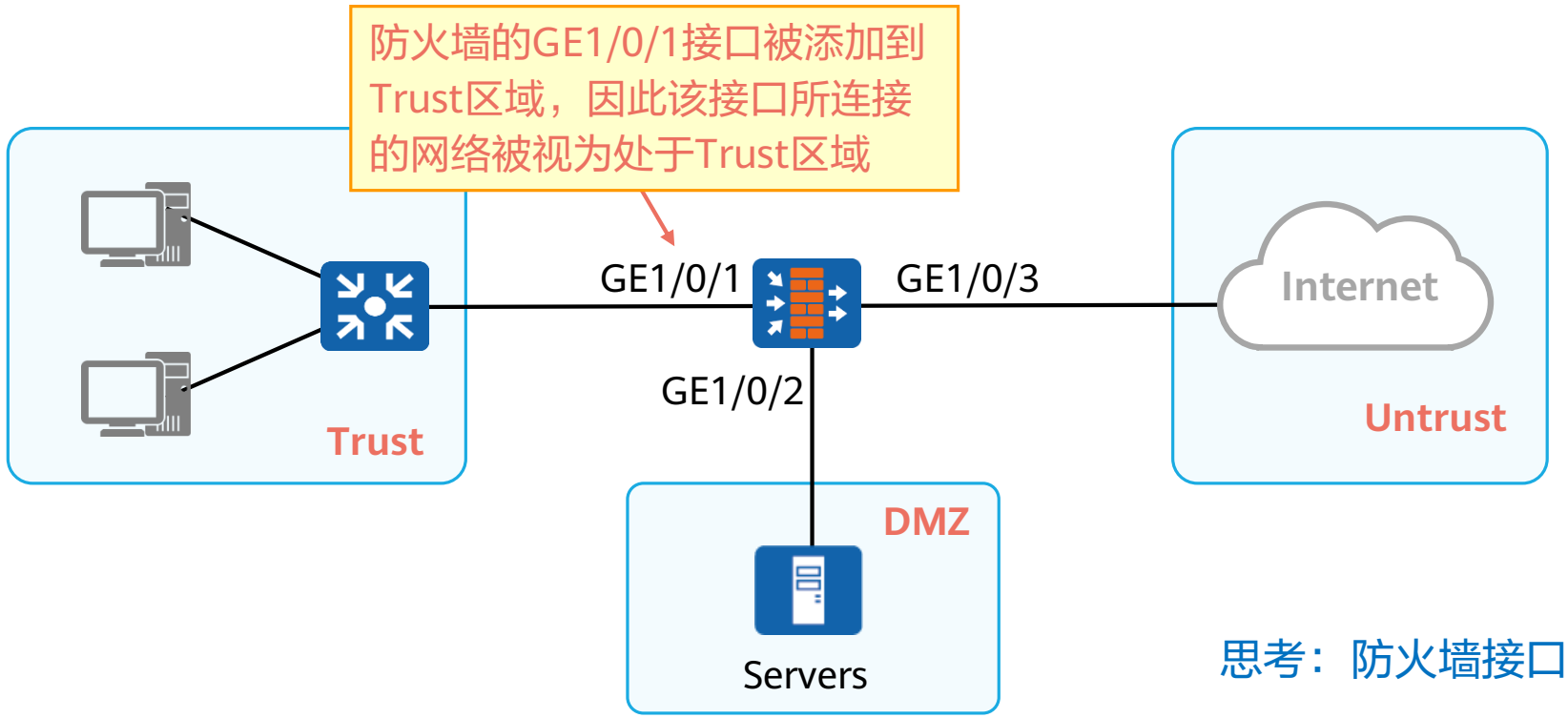


数据中心安全联动



防火墙基本概念：安全区域

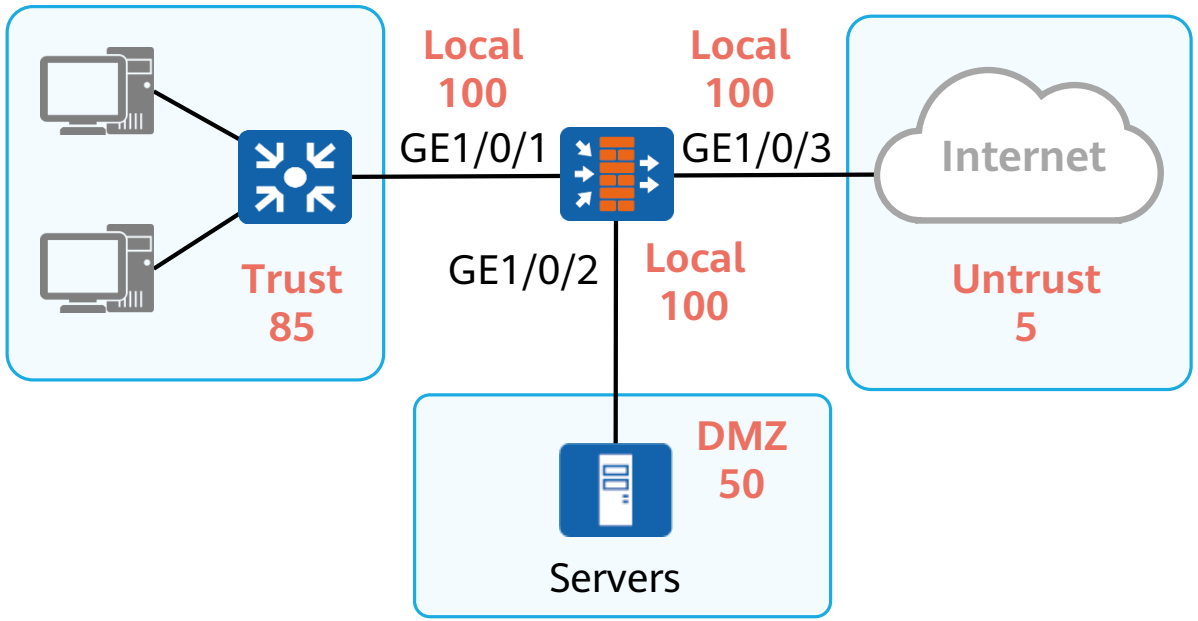
- 安全区域（Security Zone），简称为区域（Zone），是防火墙的重要概念。防火墙大部分的安全策略都基于安全区域实施。
- 一个安全区域是防火墙若干接口所连网络的集合，一个区域内的用户具有相同的安全属性。



思考：防火墙接口属于安全区域吗?

默认安全区域

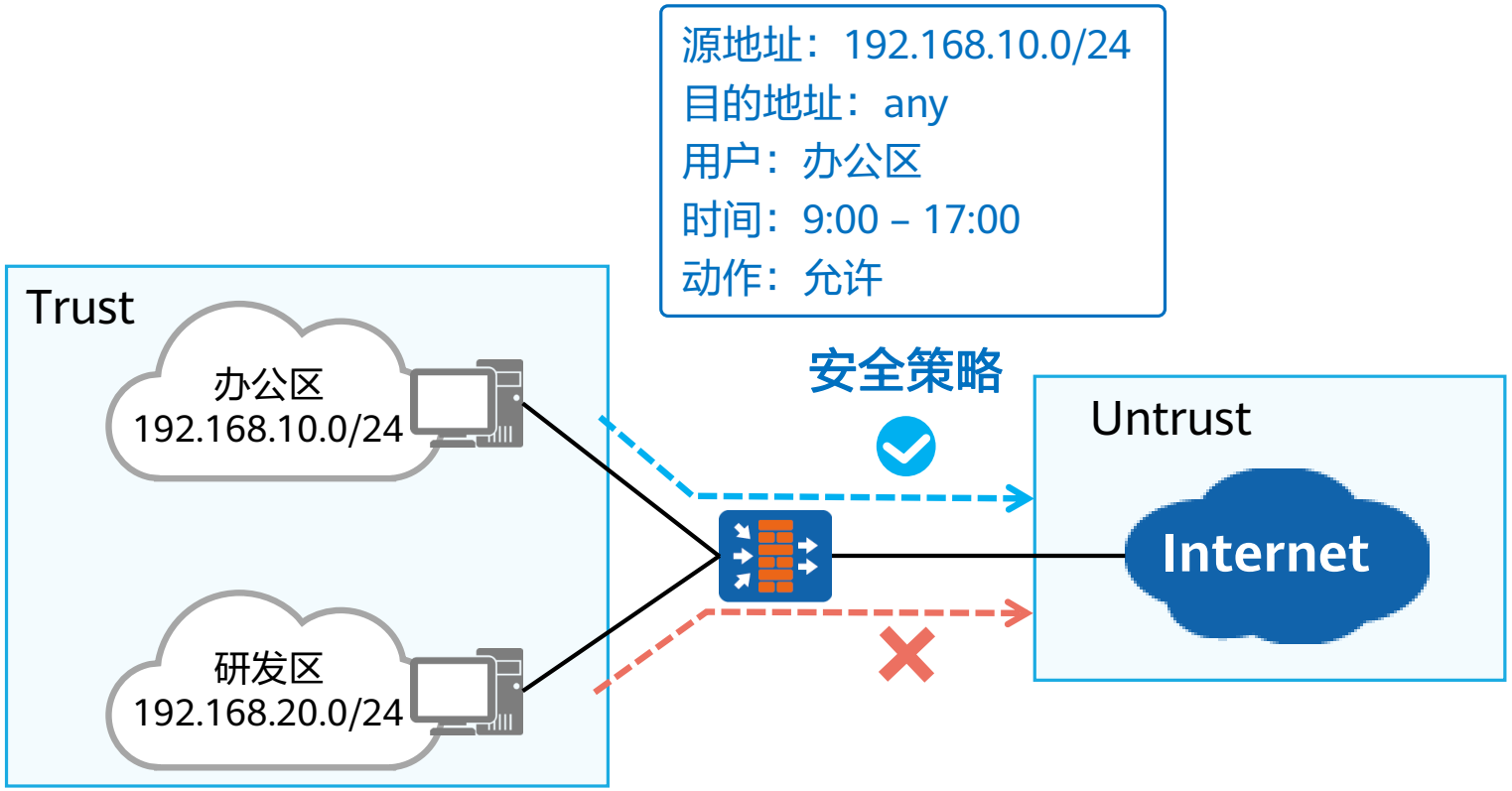
- 华为防火墙确认已创建四个区域，Untrust、DMZ、Trust和Local区域。安全区域有以下特性：
  - 默认的安全区域不能删除，也不允许修改安全级别。
  - 每个Zone都必须设置一个安全级别（Priority），值越大，则Zone的安全级别越高。
  - 用户可根据自己的需求创建自定义的Zone。



区域名称	默认安全优先级
非受信区域（Untrust）	低安全级别区域，优先级为5。
非军事化区域（DMZ）	中等安全级别区域，优先级为50。
受信区域（Trust）	较高安全级别区域，优先级为85。
本地区域（Local）	Local区域定义的是设备本身，例如设备的接口。Local区域是最高安全级别区域，优先级为100。

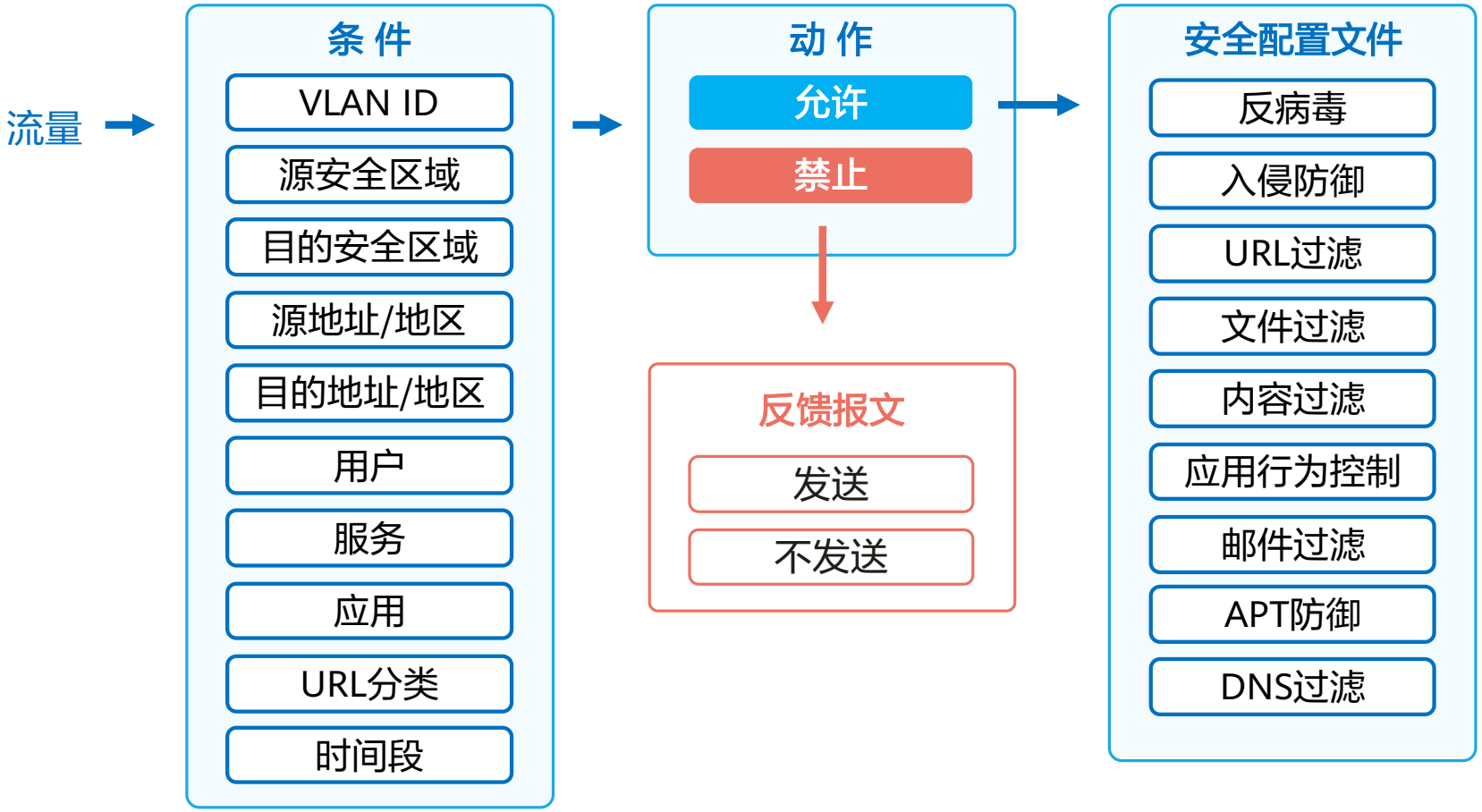
防火墙基本概念：安全策略

- 安全策略是控制防火墙对流量转发以及对流量进行内容安全一体化检测的策略。
- 当防火墙收到流量后，对流量的属性（五元组、用户、时间段等）进行识别，然后与安全策略的条件进行匹配。如果条件匹配，则此流量被执行对应的动作。



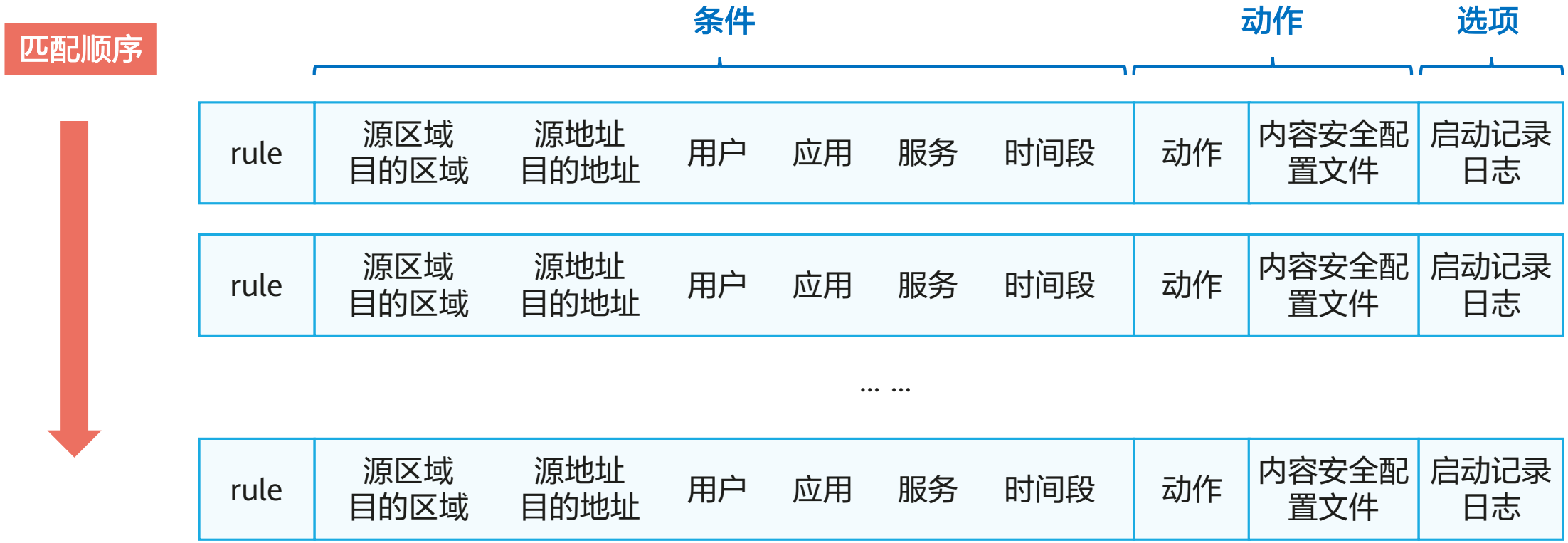
安全策略组成

- 安全策略的组成有匹配条件、动作和安全配置文件（可选）。安全配置文件实现内容安全。
- 安全策略动作如果为“允许”则可配置安全配置文件，如果为“禁止”则可配置反馈报文。



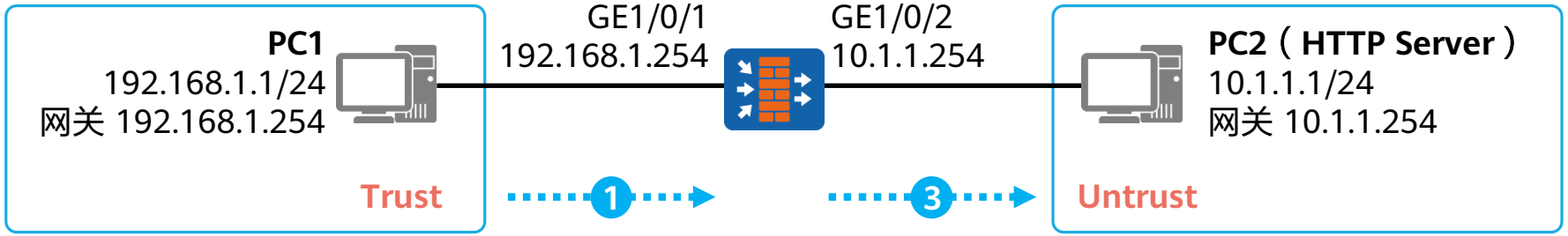
安全策略的匹配过程

- 当配置多条安全策略规则时，安全策略的匹配按照策略列表的顺序执行的，即从策略列表顶端开始逐条向下匹配。如果流量匹配了某个安全策略，将不再进行下一个策略的匹配。
- 安全策略的配置顺序很重要，需要先配置条件精确的策略，再配置宽泛的策略。



防火墙基本概念：会话表

- 会话表是用来记录TCP、UDP、ICMP等协议连接状态的表项，是FW转发报文的重要依据。
- 防火墙采用了基于“状态”的报文控制机制：只对首包或者少量报文进行检测就确定一条连接的状态，大量报文直接根据所属连接的状态进行控制。这种状态检测机制迅速提高了防火墙的检测和转发效率。会话表就是为了记录连接的状态而存在的。设备在转发TCP、UDP和ICMP报文时都需要查询会话表，来判断该报文所属的连接以及采取相应的处理措施。



1. PC1发送报文。

[FW] display firewall session table
http VPN:public --> public 192.168.1.1:52754-->10.1.1.1:80

2. 首包到达防火墙，通过会话表创建流程后，防火墙创建Session表项。

3. 防火墙放行首包。

4. PC2回复报文。

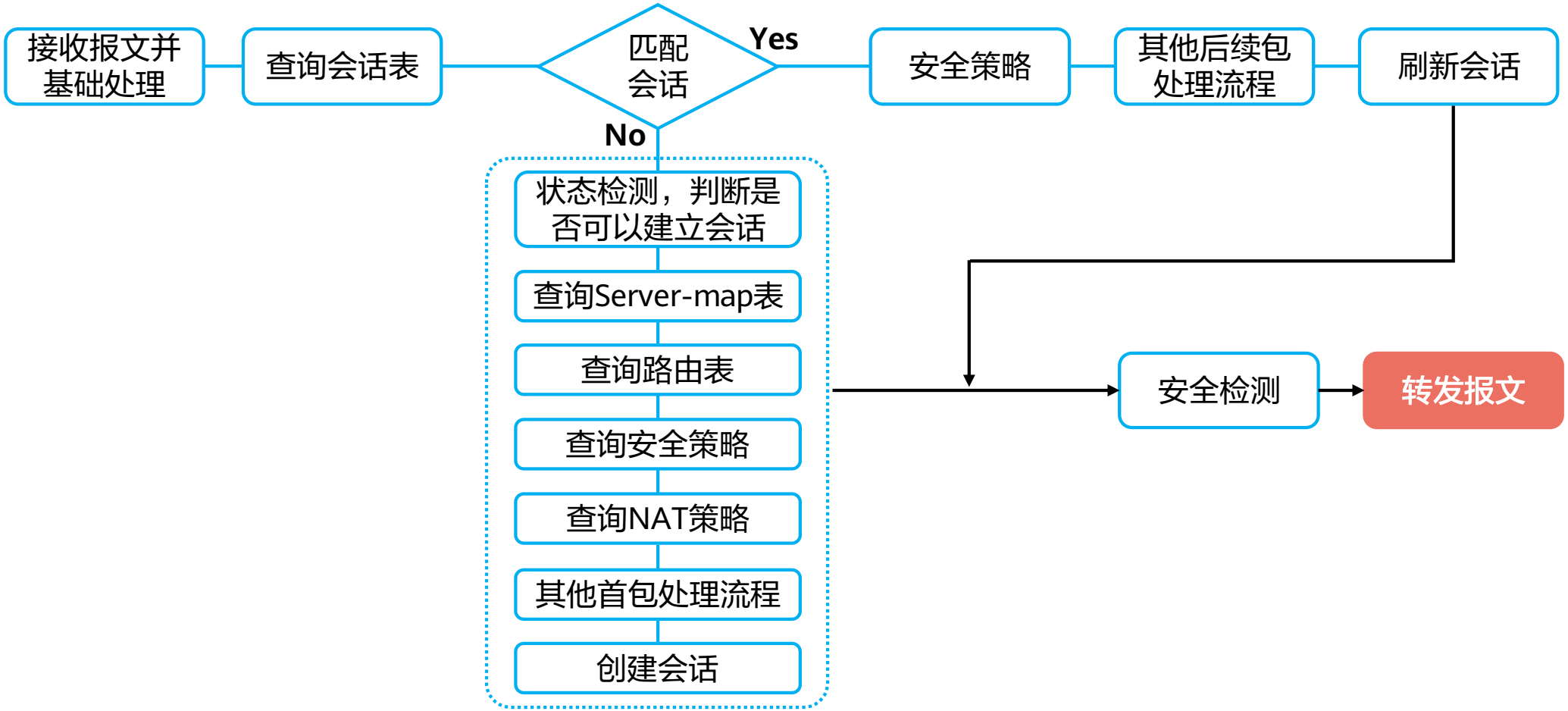
5. 回程报文匹配Session表项。

6. 防火墙转发。

[FW] display firewall session table
http VPN:public --> public 192.168.1.1:52754-->10.1.1.1:80

会话表的创建和包处理过程

- 防火墙状态检测开启情况下，流量的首包会创建会话表，后续包即可直接匹配会话表。



防火墙基础配置 - 接口

1. 创建接口/进入接口视图

[Huawei] **interface** *interface-type interface-number*

和交换机、路由器相同，interface命令用来创建接口或进入指定的接口视图。
防火墙默认为三层接口，支持使用portswitch命令切换到二层模式。

2. （接口视图）配置接口允许通过的协议

[Huawei-GigabitEthernet0/0/1] **service-manage { http | https | ping | ssh | snmp | netconf | telnet | all } { permit | deny }**

service-manage命令用来允许或拒绝管理员通过HTTP、HTTPS、Ping、SSH、SNMP、NETCONF以及Telnet访问设备。
缺省情况下，接口开启了访问控制管理功能。仅有管理接口下 HTTP、HTTPS、Ping权限放开。非管理口所有权限都关闭。此时，即使配置了接口所在安全域允许访问local区域的安全策略，也不能通过该接口访问设备。

防火墙基础配置 - 安全区域

1. 创建安全区域

[Huawei] **firewall zone name** *zone-name [* **id** *id]*

firewall zone name命令用来创建安全区域，并进入安全区域视图。id表示安全区域ID，取值4～99，默认递增。firewall zone命令用来并进入安全区域视图。防火墙默认的四个区域无需创建也不能删除。

2. （安全区域视图）设置安全区域优先级

[Huawei-zone-*name*] **set priority** *security-priority*

set priority命令用来配置安全区域的优先级。优先级取值范围为1～100，全局唯一，值越大优先级越高。系统默认的安全区域不能被删除，优先级也无法被重新配置或者删除。

3. （安全区域视图）添加接口到安全区域

[Huawei] **add interface** *interface-type { interface-number | interface-number.subinterface-number }*

add interface命令用来将接口加入到安全区域。安全区域在使用时需要与FW的特定接口相关联，即需要将接口加入到安全区域。该接口既可以是物理接口，也可以是逻辑接口。

防火墙基础配置 - 安全策略 (1)

1. 进入安全策略视图

```
[Huawei] security-policy
```

security-policy命令用来进入安全策略视图。安全策略规则的创建、复制、移动和重命名都在此视图下完成。

2. （安全策略视图）配置接口允许通过的协议

```
[Huawei-policy-security] rule name rule-name
```

rule name命令用来创建安全策略规则，并进入安全策略规则视图。

3. （安全策略规则视图）配置安全策略规则的源安全区域

```
[Huawei-policy-security-rule-name] source-zone { zone-name &<1-6> | any }
```

source-zone命令用来配置安全策略规则的源安全区域。命令中zone-name必须为系统已经存在的安全区域名称。安全策略规则一次最多添加或删除6个安全区域。

4. （安全策略规则视图）配置安全策略规则的目的安全区域

```
[Huawei-policy-security-rule-name] destination-zone { zone-name &<1-6> | any }
```

防火墙基础配置 - 安全策略 (2)

5. （安全策略规则视图）配置安全策略规则的源IP地址

```
[Huawei-policy-security-rule-name] source-address ipv4-address { ipv4-mask-length | mask mask-address}
```

source-address命令用来配置安全策略规则的源地址。命令中mask-address使用反掩码。

6. （安全策略规则视图）配置安全策略规则的目的IP地址

```
[Huawei-policy-security-rule-name] destination-address ipv4-address { ipv4-mask-length | mask mask-address}
```

destination-address命令用来配置安全策略规则的目的地址。命令中mask-address使用反掩码。

7. （安全策略规则视图）配置安全策略规则的目的IP地址

```
[Huawei] service { service-name &<1-6> | any }
```

service命令用来配置服务，例如service protocol命令用来在安全策略中直接引用TCP/UDP/SCTP端口或IP层协议。

8. （安全策略规则视图）配置安全策略规则的目的安全区域

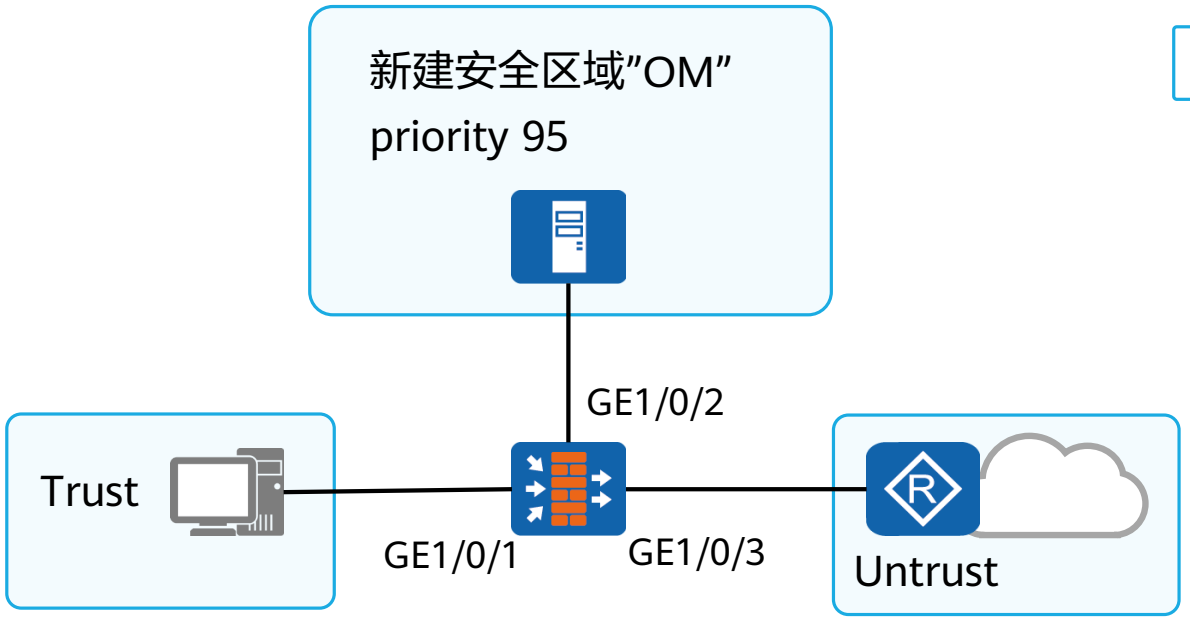
```
[Huawei] action { permit | deny }
```

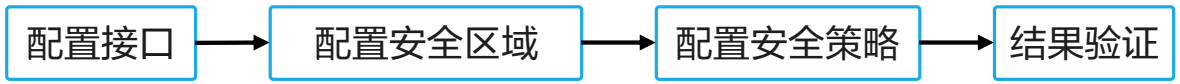
action命令用来配置安全策略规则的动作。防火墙default action deny。

防火墙配置案例

案例描述：

- 防火墙将网络隔离为三个安全区域，Trust、Untrust和OM，其中OM区域优先级为95。现有需求如下：
  - 允许防火墙接口GE1/0/1响应Ping请求。
  - 允许Untrust区域ICMP流量访问OM区域。





配置过程分为四个步骤：

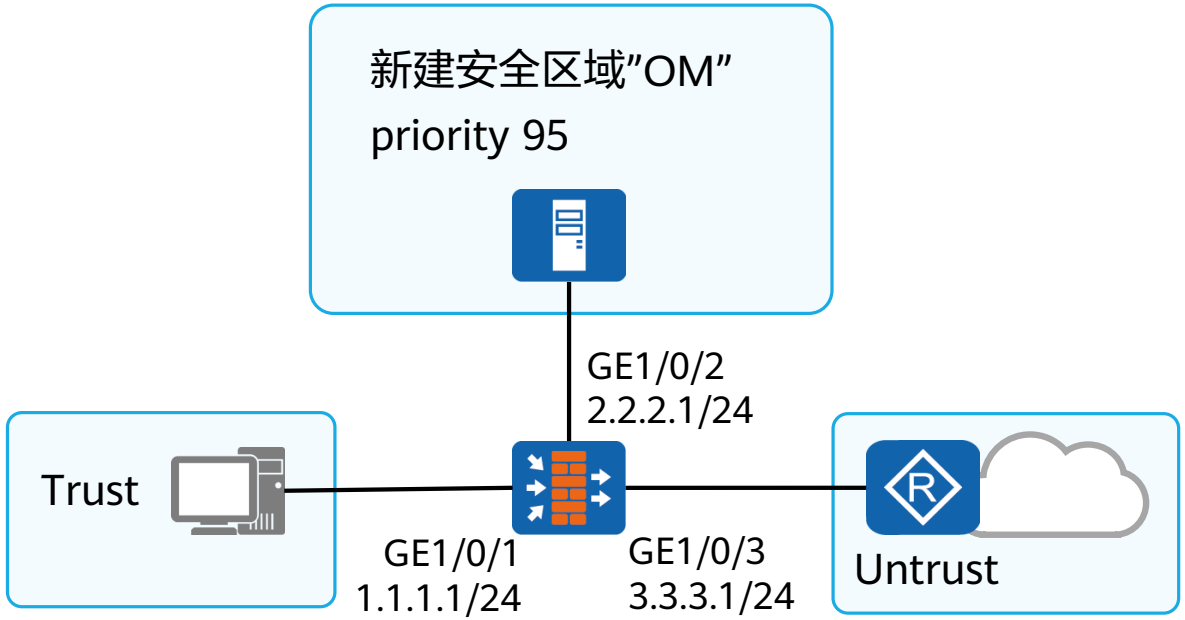
- 配置防火墙接口。
- 配置防火墙安全区域。
- 配置防火墙安全策略。
- 结果验证。

配置案例 - 接口

配置接口 → 配置安全区域 → 配置安全策略 → 结果验证

任务列表：

- 根据规划，配置防火墙接口IP地址。
- 允许GE1/0/1响应Ping服务。



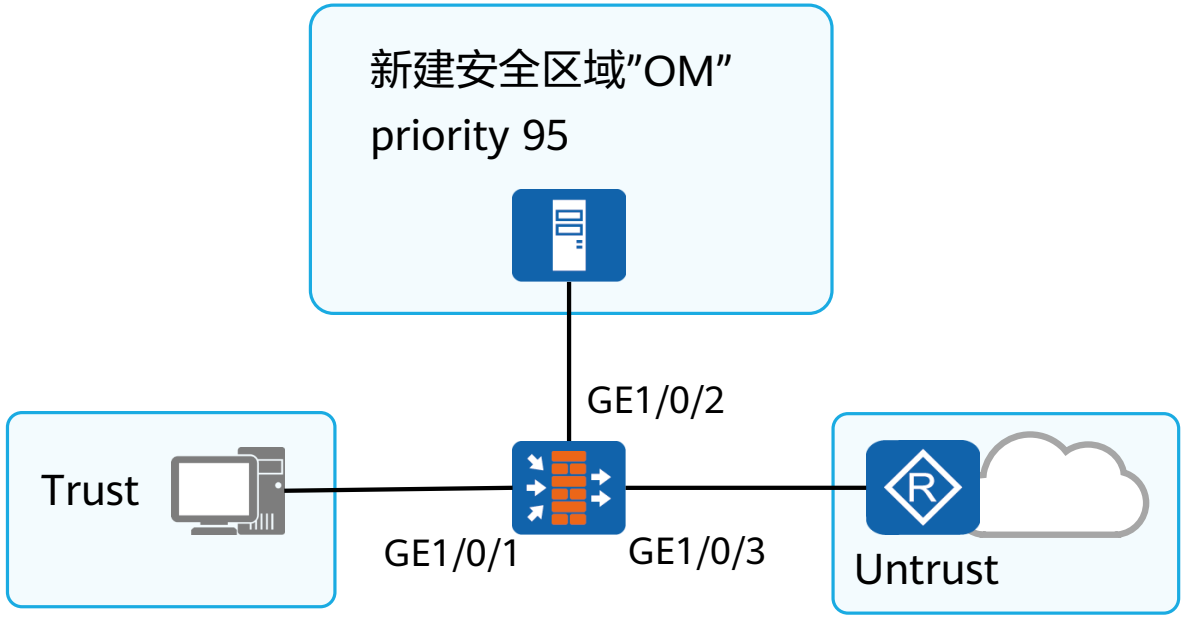

```
#配置接口IP地址并允许GE1/0/1的ping业务
[FW] interface GigabitEthernet 1/0/1
[FW-GigabitEthernet1/0/1] ip address 1.1.1.1 24
[FW-GigabitEthernet1/0/1] service-manage ping permit
[FW-GigabitEthernet1/0/1] interface GigabitEthernet 1/0/2
[FW-GigabitEthernet1/0/2] ip address 2.2.2.1 24
[FW-GigabitEthernet1/0/2] interface GigabitEthernet 1/0/3
[FW-GigabitEthernet1/0/3] ip address 3.3.3.1 24
```

配置案例 - 安全区域

配置接口 → **配置安全区域** → 配置安全策略 → 结果验证

任务列表：

- 防火墙新建安全区域“OM”，其优先级为95。
- 将接口划分入规划的安全区域。



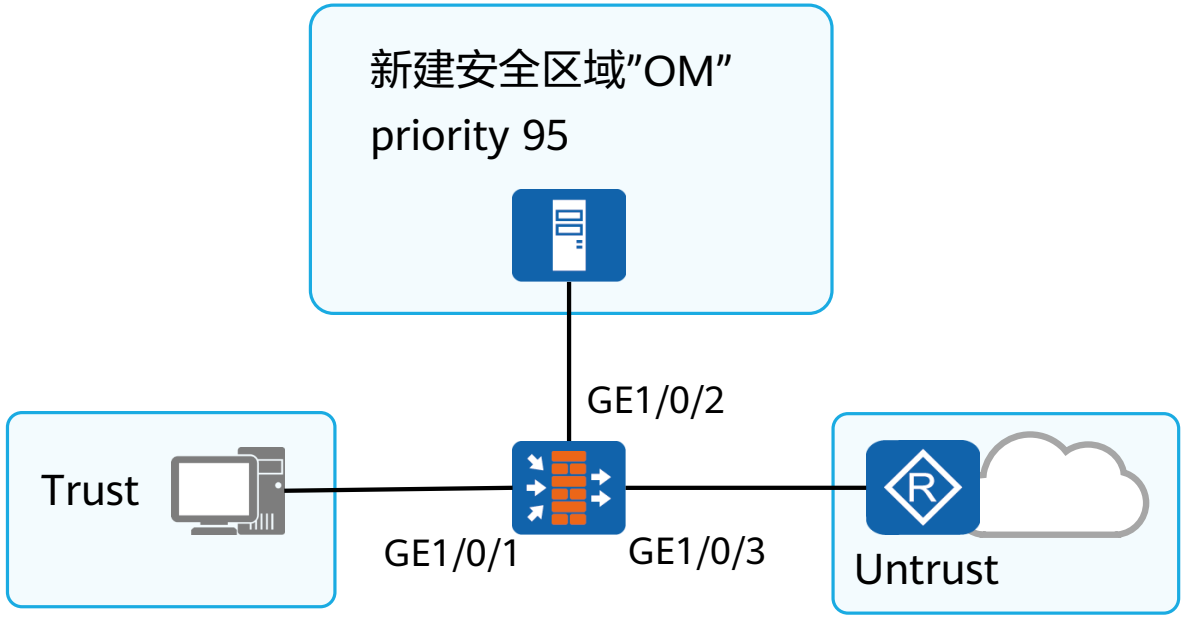

```
#创建安全区域
[FW] firewall zone name OM
[FW-zone-OM] set priority 95
[FW-zone-OM] quit

#将接口添加到安全区域：
[FW] firewall zone trust
[FW-zone-trust] add interface GigabitEthernet 1/0/1
[FW] firewall zone OM
[FW-zone-OM] add interface GigabitEthernet 1/0/2
[FW] firewall zone untrust
[FW-zone-untrust] add interface GigabitEthernet 1/0/3
```

配置案例 - 安全策略

配置接口 → 配置安全区域 → **配置安全策略** → 结果验证

任务列表：

- 创建安全策略R1
- 配置安全策略规则，配置源目的区域、业务类型和行为。

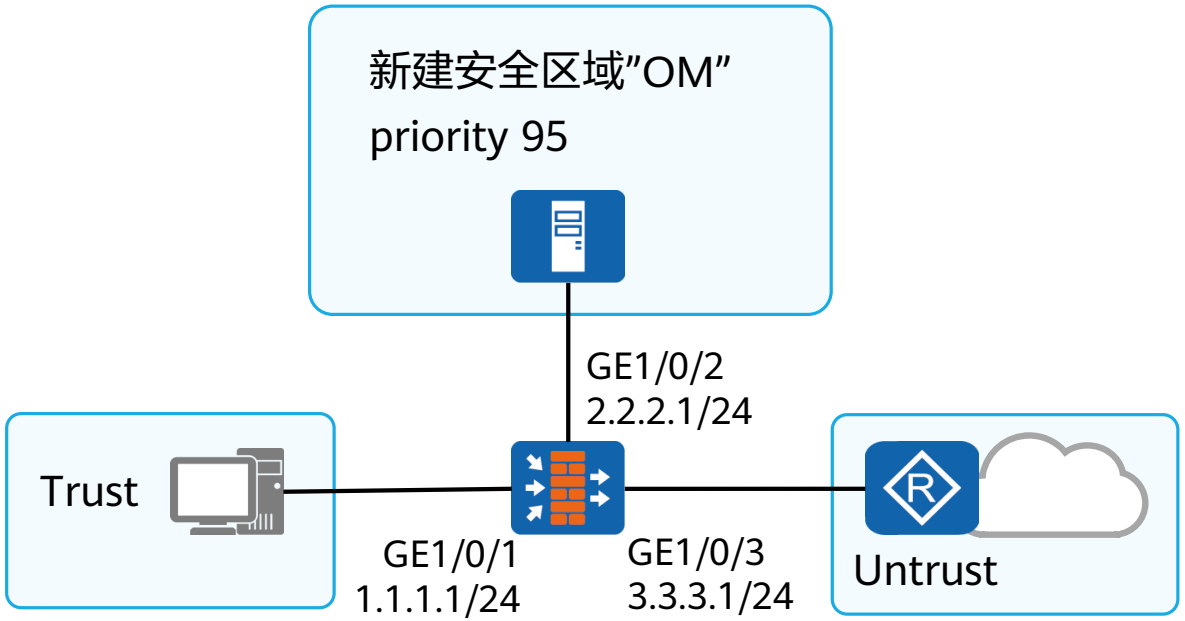



```
#创建安全策略
[FW-policy-security] rule name R1
[FW-policy-security-rule-R1] source-zone untrust
[FW-policy-security-rule-R1] destination-zone OM
[FW-policy-security-rule-R1] service icmp
[FW-policy-security-rule-R1] action permit
```

配置案例 - 结果验证 (1)

配置接口 → 配置安全区域 → 配置安全策略 → **结果验证**

1. Trust区域内PC向防火墙GE1/0/1接口发起ping测试。



#查看防火墙会话表

[FW]display firewall session table

2020-03-11 10:31:21.010

Current Total Sessions : 4

icmp VPN: public --> public 1.1.1.2:14265 --> 1.1.1.1:2048

icmp VPN: public --> public 1.1.1.2:15289 --> 1.1.1.1:2048

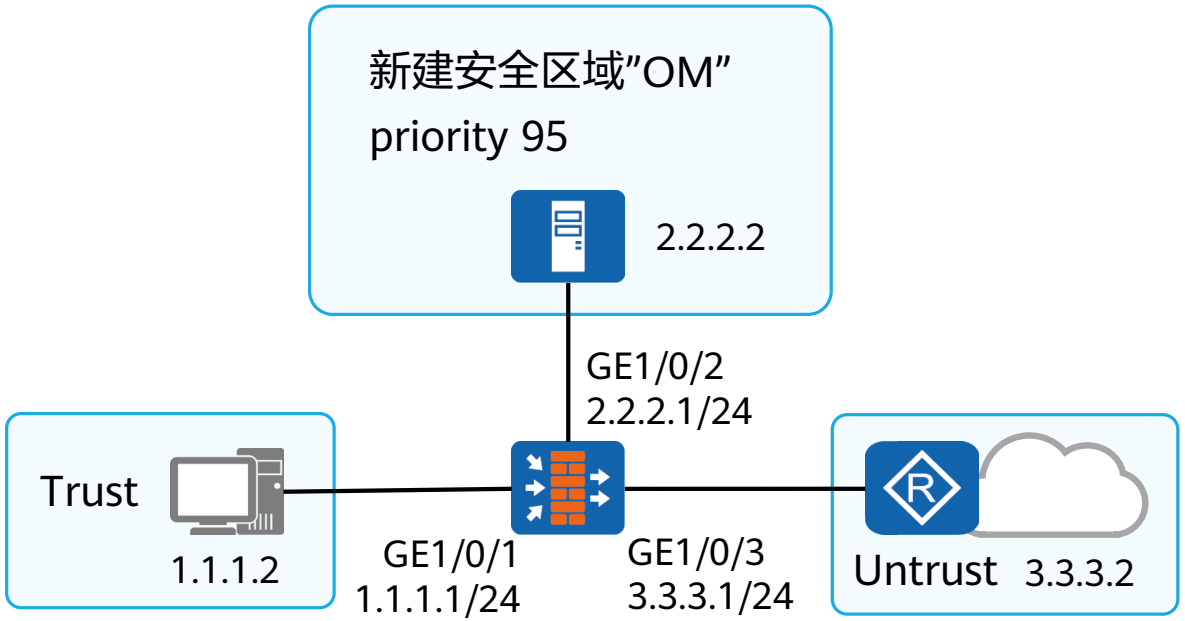
icmp VPN: public --> public 1.1.1.2:14777 --> 1.1.1.1:2048

icmp VPN: public --> public 1.1.1.2:15033 --> 1.1.1.1:2048

配置案例 - 结果验证 (2)

配置接口 → 配置安全区域 → 配置安全策略 → **结果验证**

2. Untrust区域3.3.3.2向OM区域2.2.2.2发起ping测试。




```
#查看防火墙会话表
[FW]display firewall session table
2020-03-11 10:30:15.150
 Current Total Sessions : 4
 icmp  VPN: public --> public  3.3.3.2:63928 --> 2.2.2.2:2048
 icmp  VPN: public --> public  3.3.3.2:63672 --> 2.2.2.2:2048
 icmp  VPN: public --> public  3.3.3.2:63416 --> 2.2.2.2:2048
 icmp  VPN: public --> public  3.3.3.2:62904 --> 2.2.2.2:2048
```

思考题

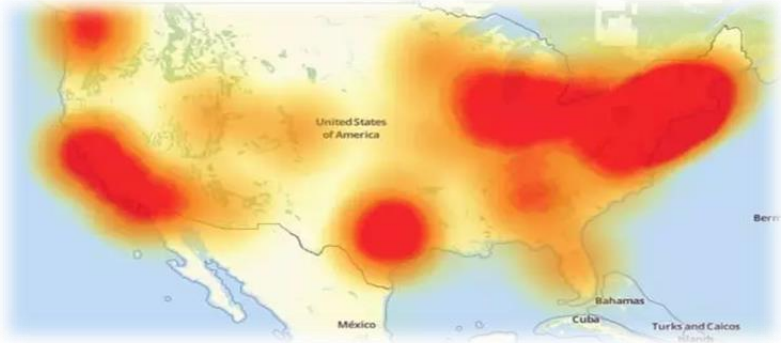
1. （单选）缺省情况下，防火墙有几个安全区域？（　　）

A. 1　　B. 2　　C. 3　　D. 4

目录

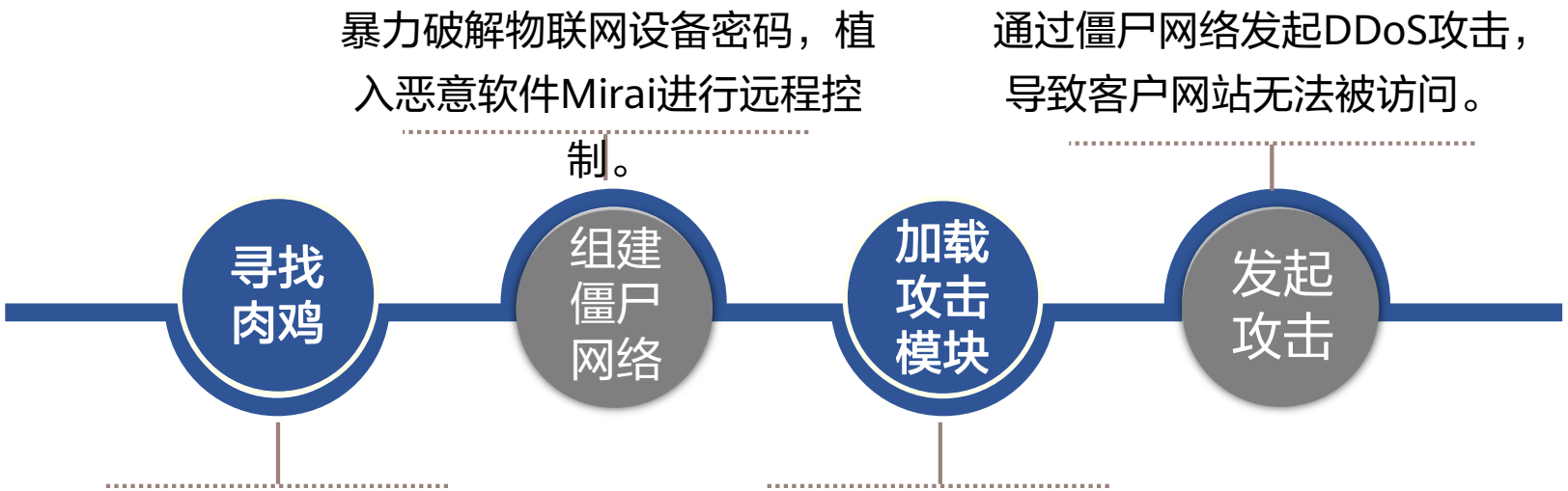
美国Dyn DNS服务遭受DDoS攻击

- 2016年10月21日11点-17点（UTC时间），美国Dyn DNS服务遭受DDoS攻击事件，近半个美国陷入断网。
- 此次大规模DDoS攻击是由物联网设备所组成的僵尸网络所发动的，这些设备感染了Mirai恶意软件。



发起攻击的物联网设备

Mirai病毒发动攻击的过程



本次攻击用到了哪些方法?

扫描

- 扫描是一种潜在的攻击行为，本身并不具有直接的破坏行为，通常是攻击者发动真正攻击前的网络探测行为。

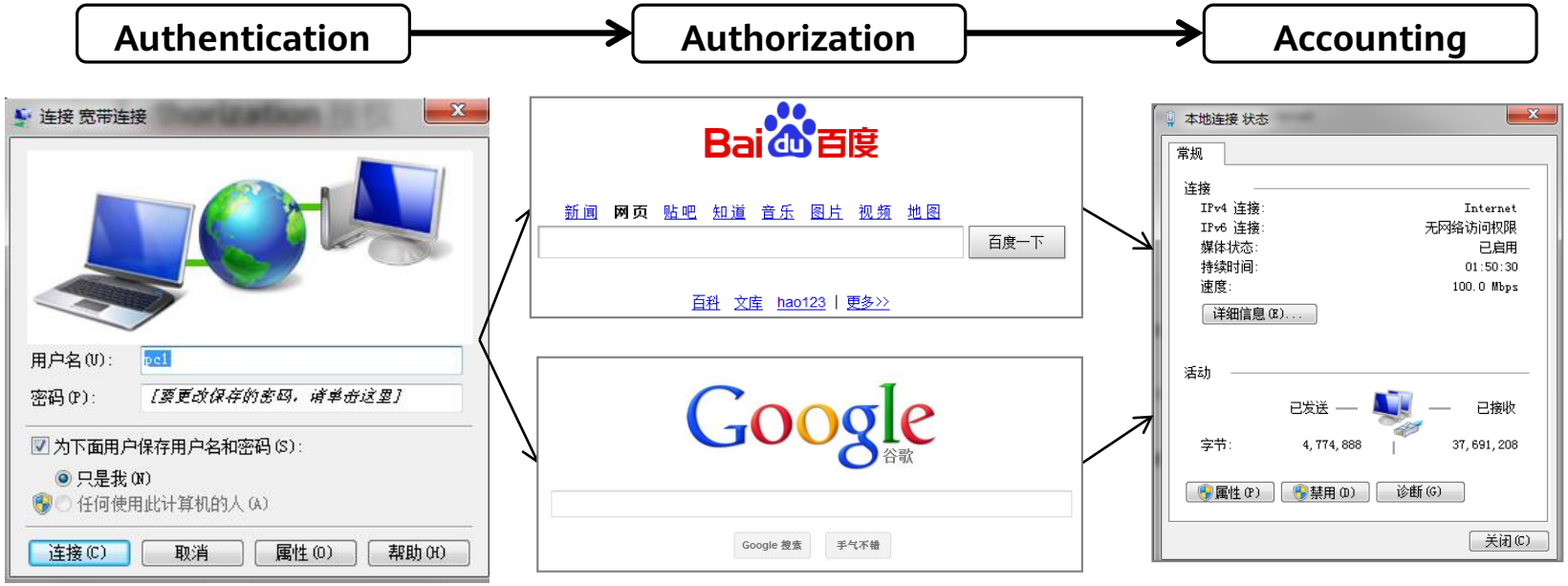
地址扫描	端口扫描
攻击者运用ICMP报文探测目标地址，或者使用TCP/UDP报文对一定地址发起连接，通过判断是否有应答报文，以确定哪些目标系统确实存活着并且连接在目标网络上。	攻击者通过对端口进行扫描探寻被攻击对象目前开放的端口，以确定攻击方式。在端口扫描攻击中，攻击者通常使用Port Scan攻击软件，发起一系列TCP/UDP连接，根据应答报文判断主机是否使用这些端口提供服务。

防御方法：在防火墙上开启扫描防御功能，当检测到扫描频率超过阈值时，将源IP加入黑名单。

用户认证的背景

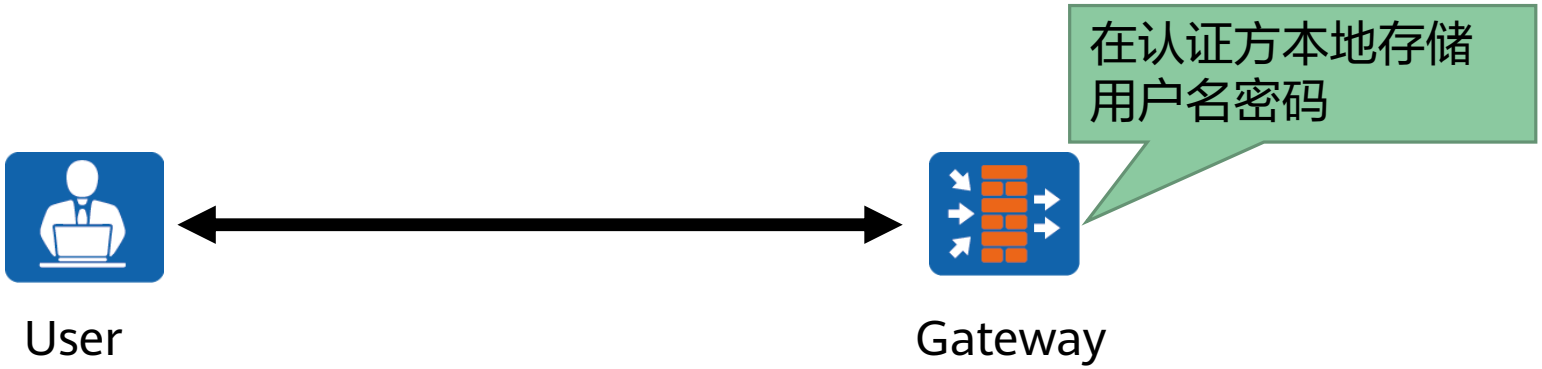
什么是AAA

- Authentication认证
- Authorization 授权
- Accounting 计费

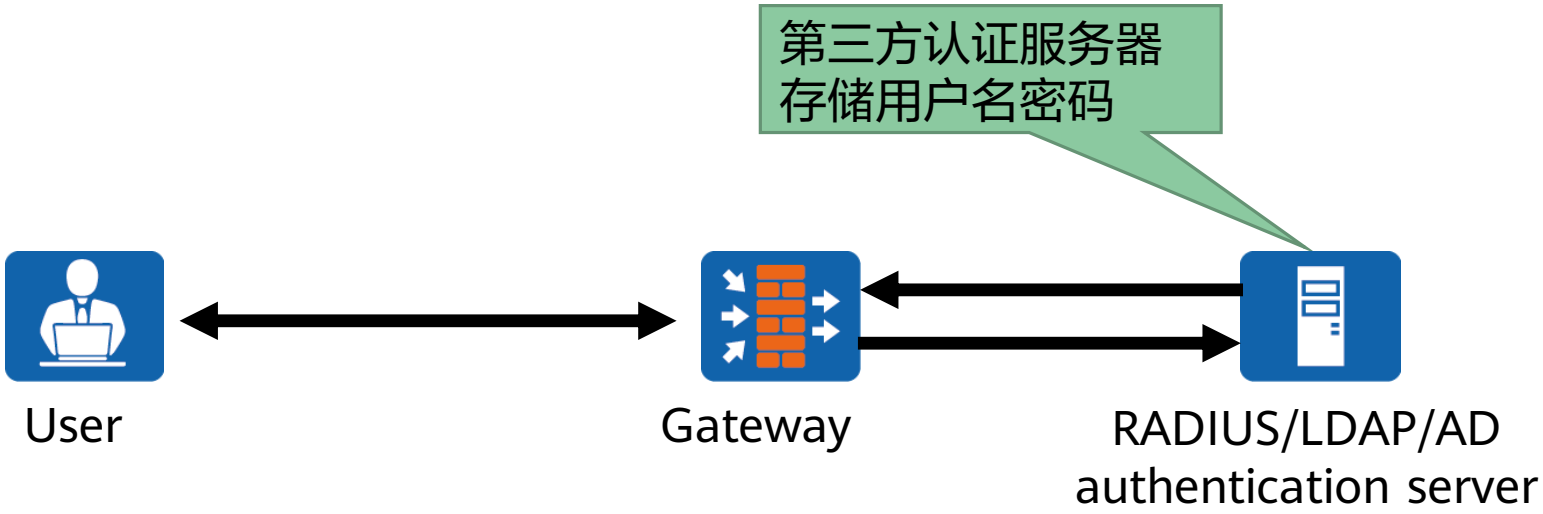


AAA技术

- 本地认证



- 服务器认证

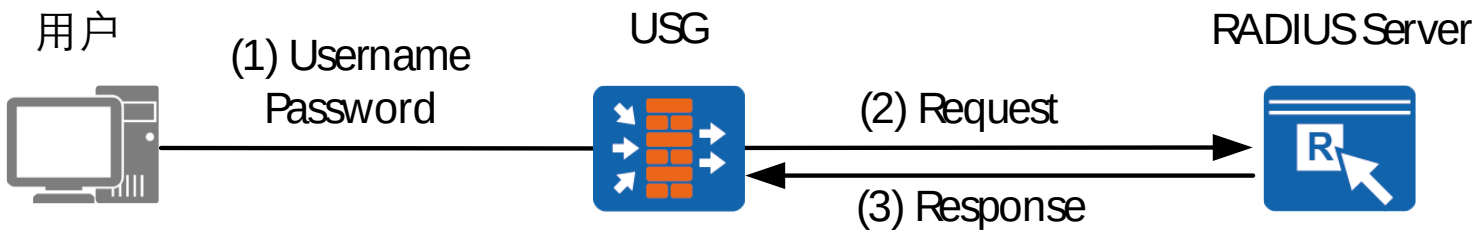


用户组织架构

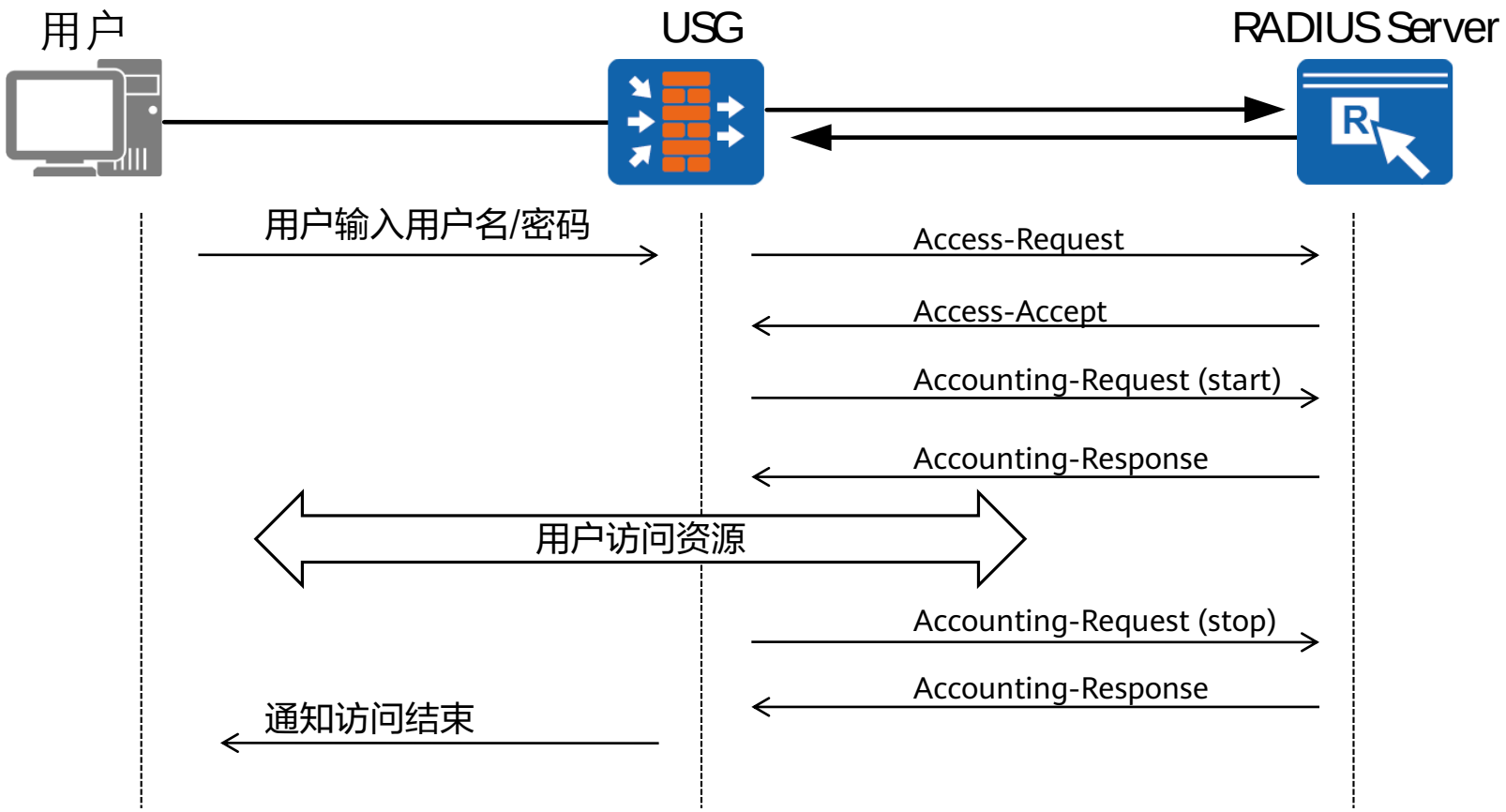
- 用户是网络访问的主体，是FW进行网络行为控制和网络权限分配的基本单元。
- 用户组织结构中涉及如下三个概念：
  - 认证域：用户组织结构的容器，防火墙缺省存在default认证域，用户可以根据需求新建认证域。
  - 用户组/用户：用户按树形结构组织，用户隶属于组（部门）。管理员可以根据企业的组织结构来创建部门和用户。

RADIUS协议概述

- RADIUS服务器通过建立一个唯一的用户数据库，存储用户名、密码来对用户进行验证。



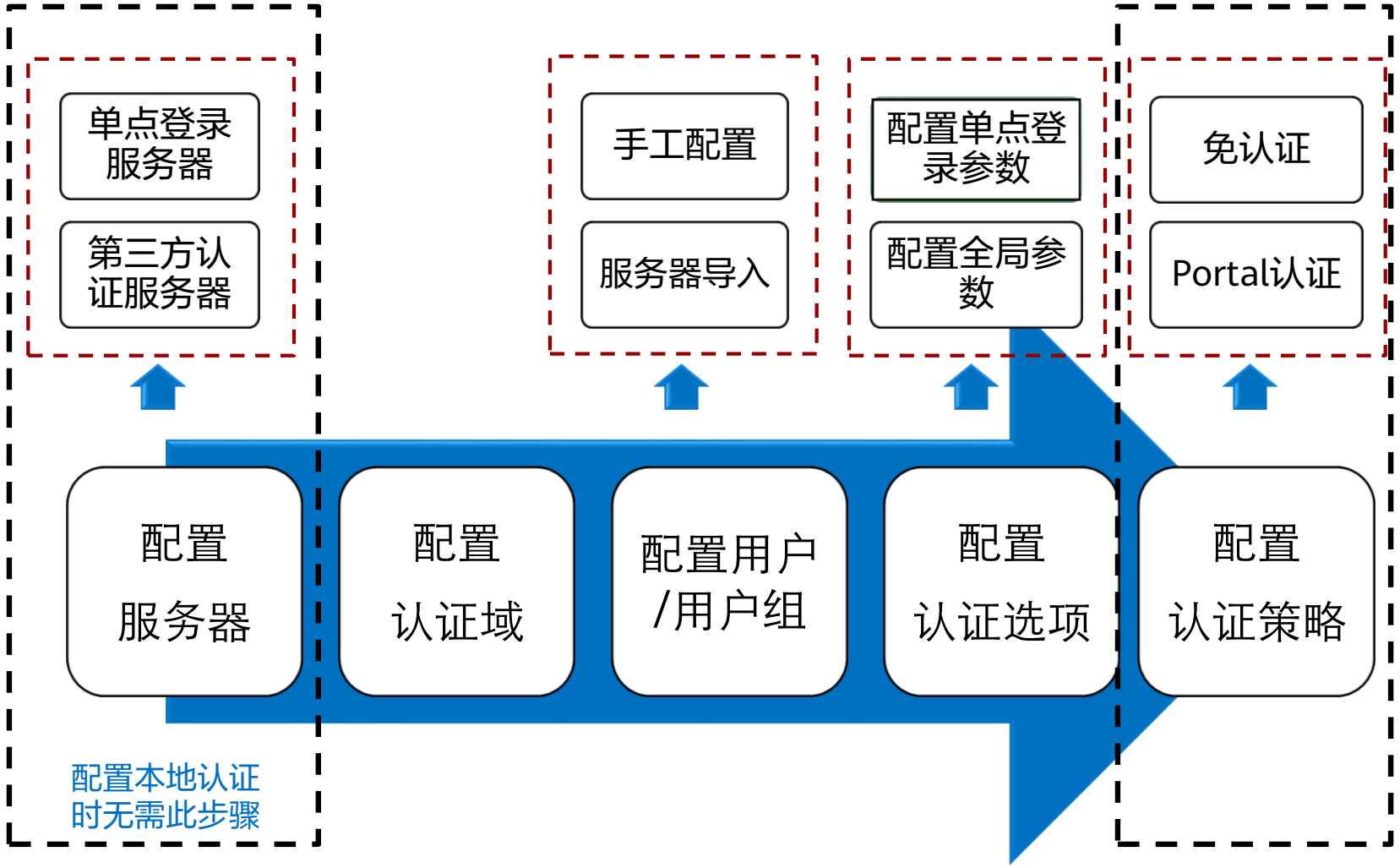
RADIUS应用场景



认证策略

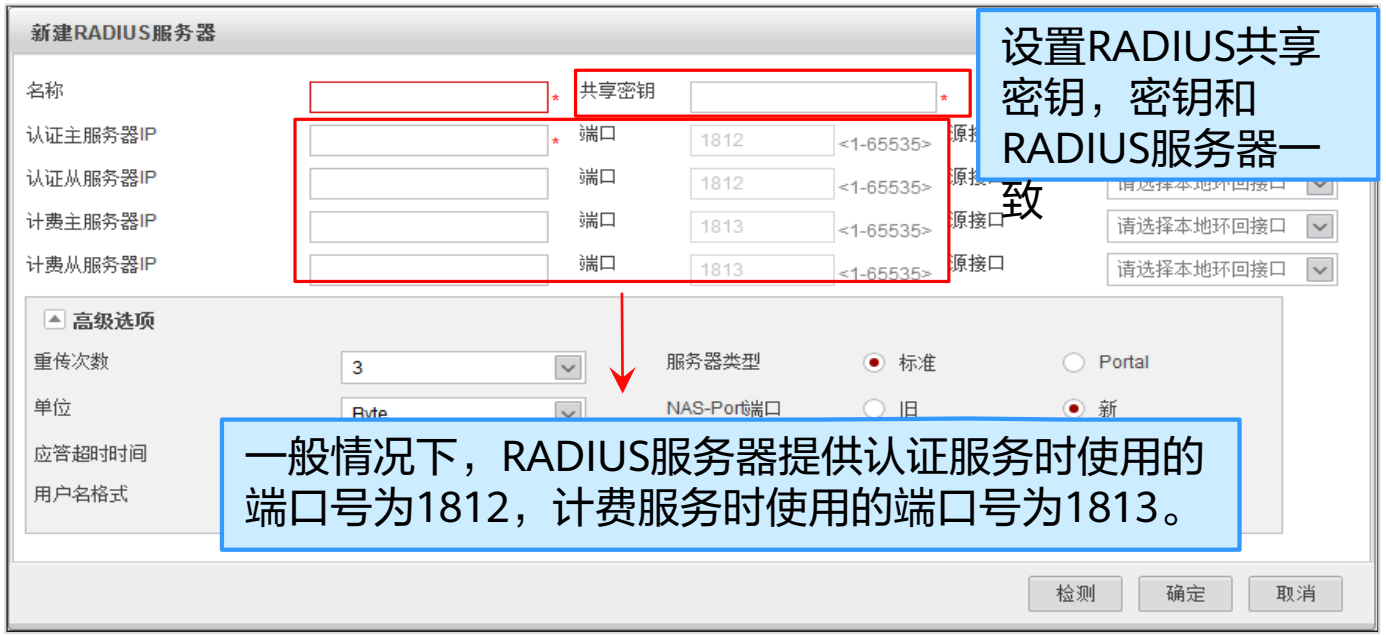
- 认证策略用于决定防火墙需要对哪些数据流进行认证，匹配认证策略的数据流必须经过防火墙的身份认证才能通过。认证策略是多个认证策略规则的集合，认证策略决定是否对一条流量进行认证。认证策略规则由条件和动作组成，条件指的是FW匹配报文的依据，包括：
  - 源/目的安全区域
  - 源地址/地区
  - 目的地址/地区
- 动作指的是FW对匹配到的数据流采取的处理方式，包括：

配置流程



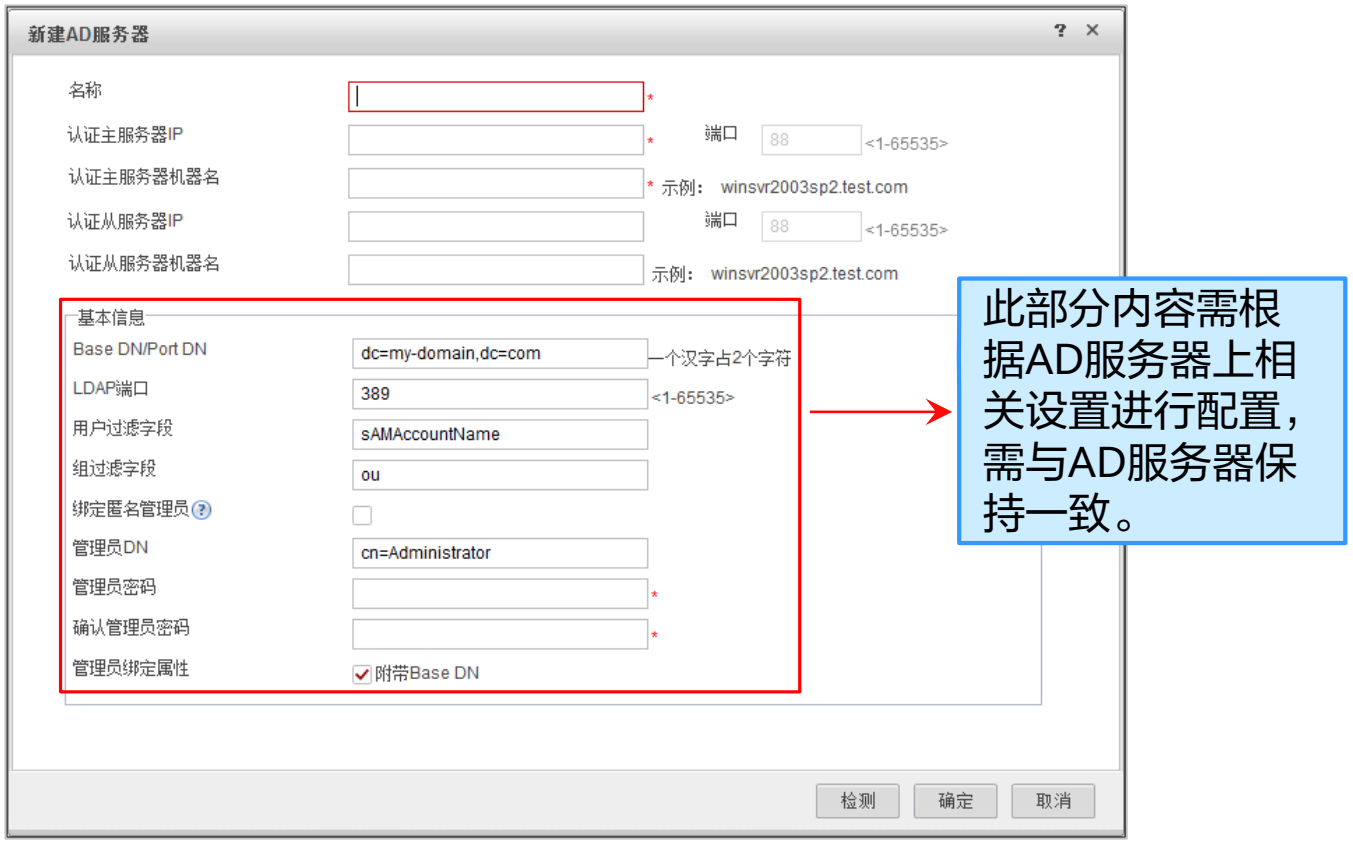
配置服务器（RADIUS）

- 在“对象> 认证服务器 > RADIUS > 新建”，新建RADIUS服务器。



配置服务器（AD）

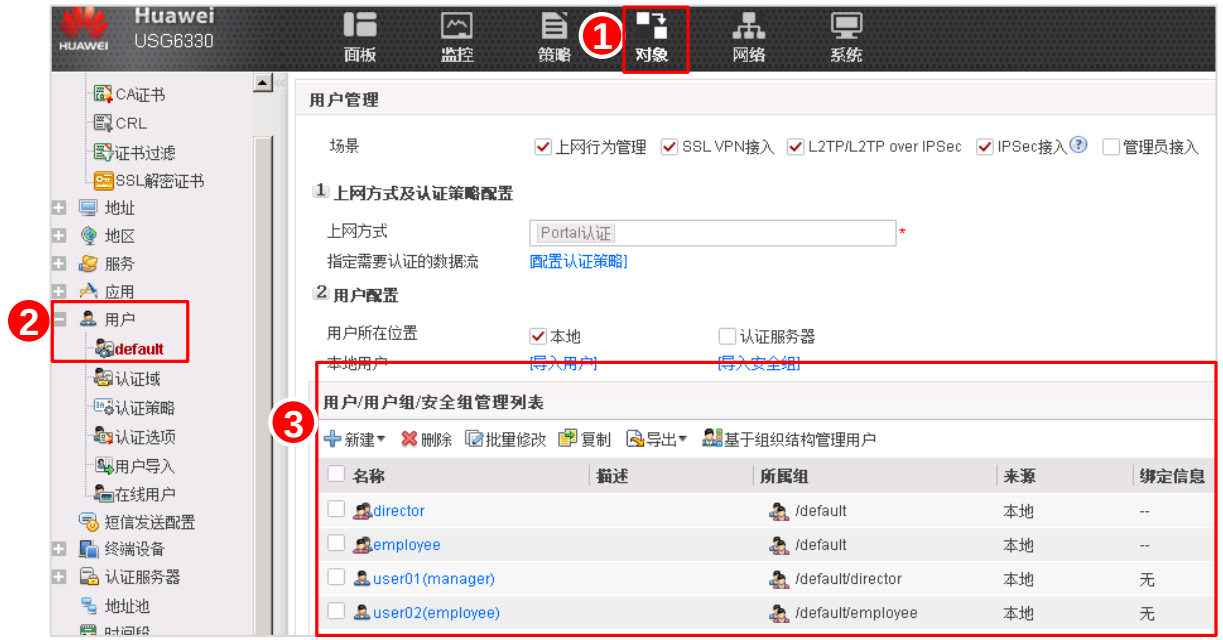
- 在“对象> 认证服务器 > AD > 新建”，新建AD服务器。



此部分内容需根据AD服务器上相关设置进行配置，需与AD服务器保持一致。

创建用户和用户组

- 在“对象> 用户 > default ”，新建用户/用户组。

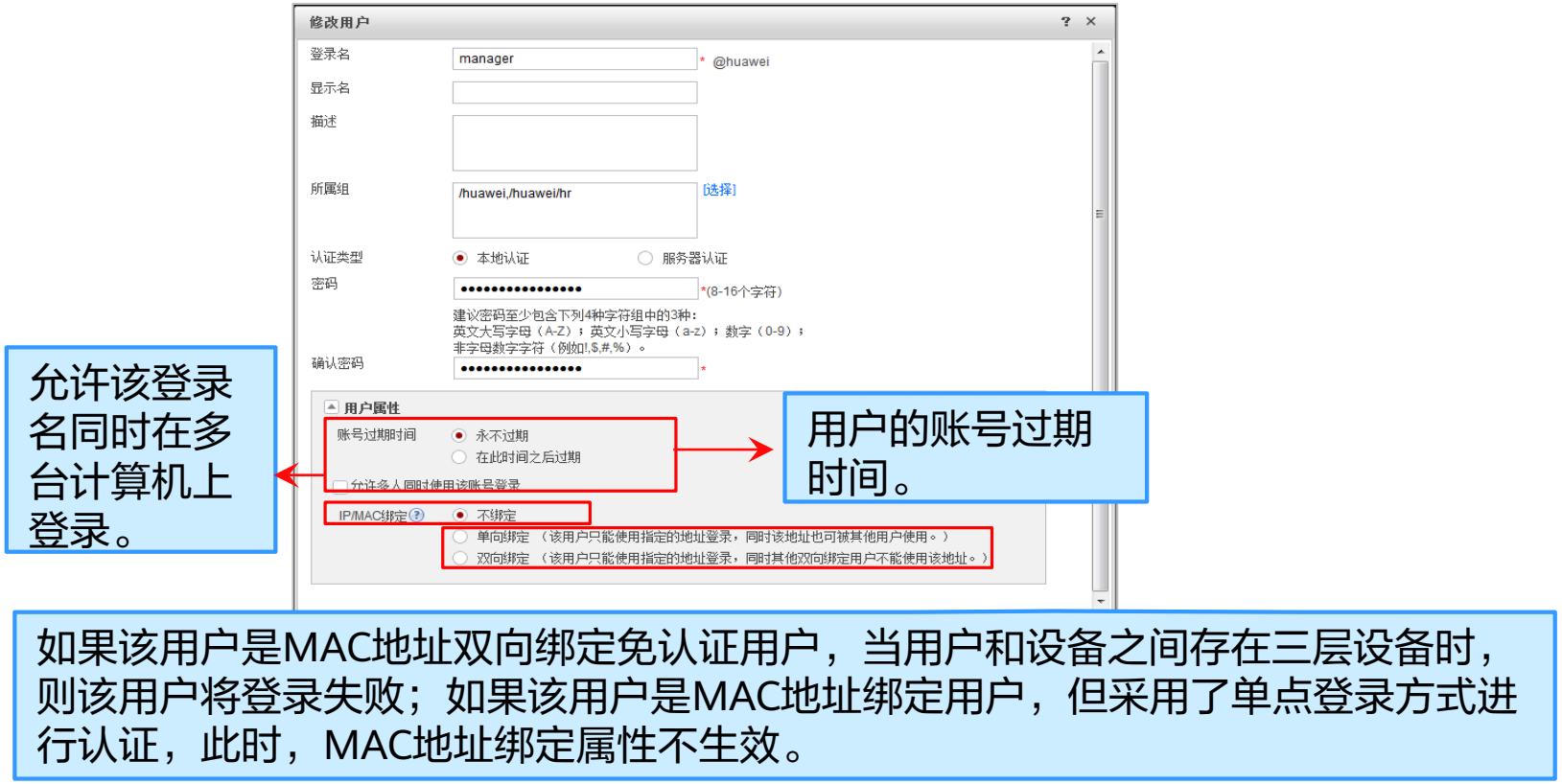


表示用户组，列表中只显示该用户组的所属组和描述信息。其他参数均显示为“--”，即表示非用户组相关参数，不可配置。

表示用户，列表中除能直接显示用户所属组、绑定信息、账号过期时间、描述信息以及当前的用户状态，还能修改用户状态。

配置用户属性

- 对于已存在的用户可以使用“编辑”修改用户的属性。



允许该登录名同时在多台计算机上登录。

用户的账号过期时间。

如果该用户是MAC地址双向绑定免认证用户，当用户和设备之间存在三层设备时，则该用户将登录失败；如果该用户是MAC地址绑定用户，但采用了单点登录方式进行认证，此时，MAC地址绑定属性不生效。

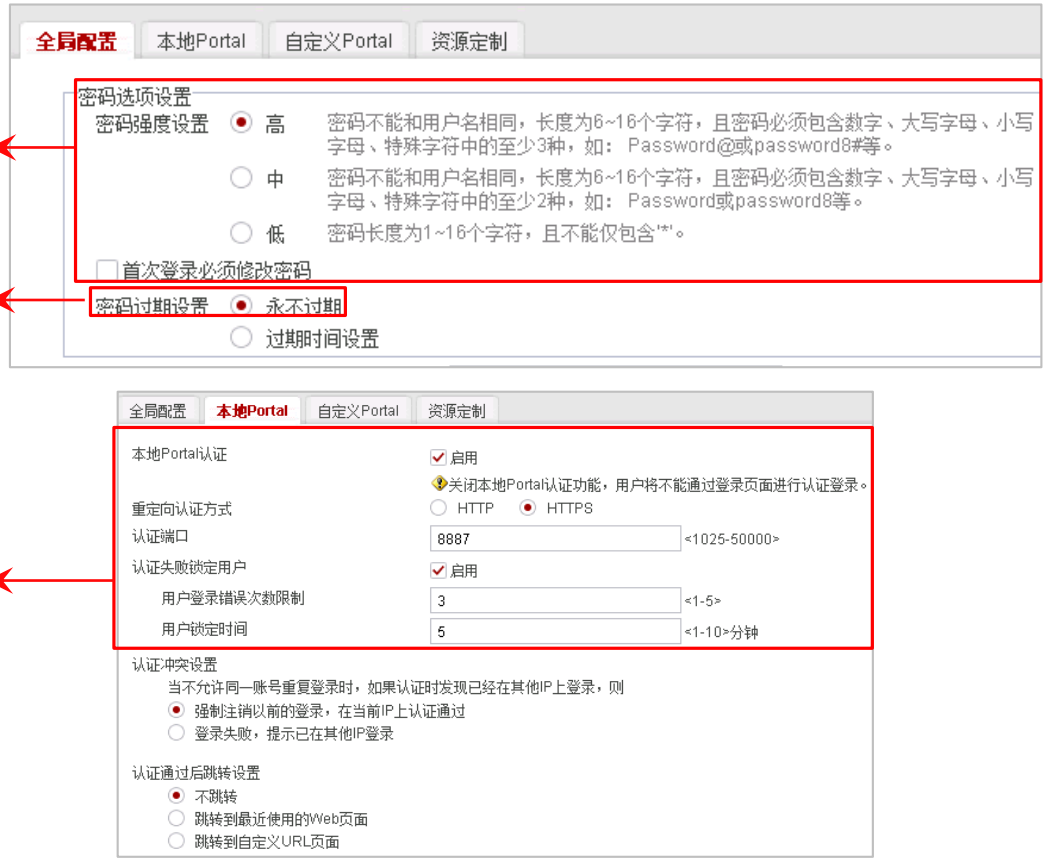
配置认证选项 (全局配置)

- 在“对象> 用户 > 认证选项 > 全局配置/本地Portal”，进行配置。

用户可在登录认证页面时对密码进行修改，且该配置只适用于用户通过认证页面来修改密码的情况。

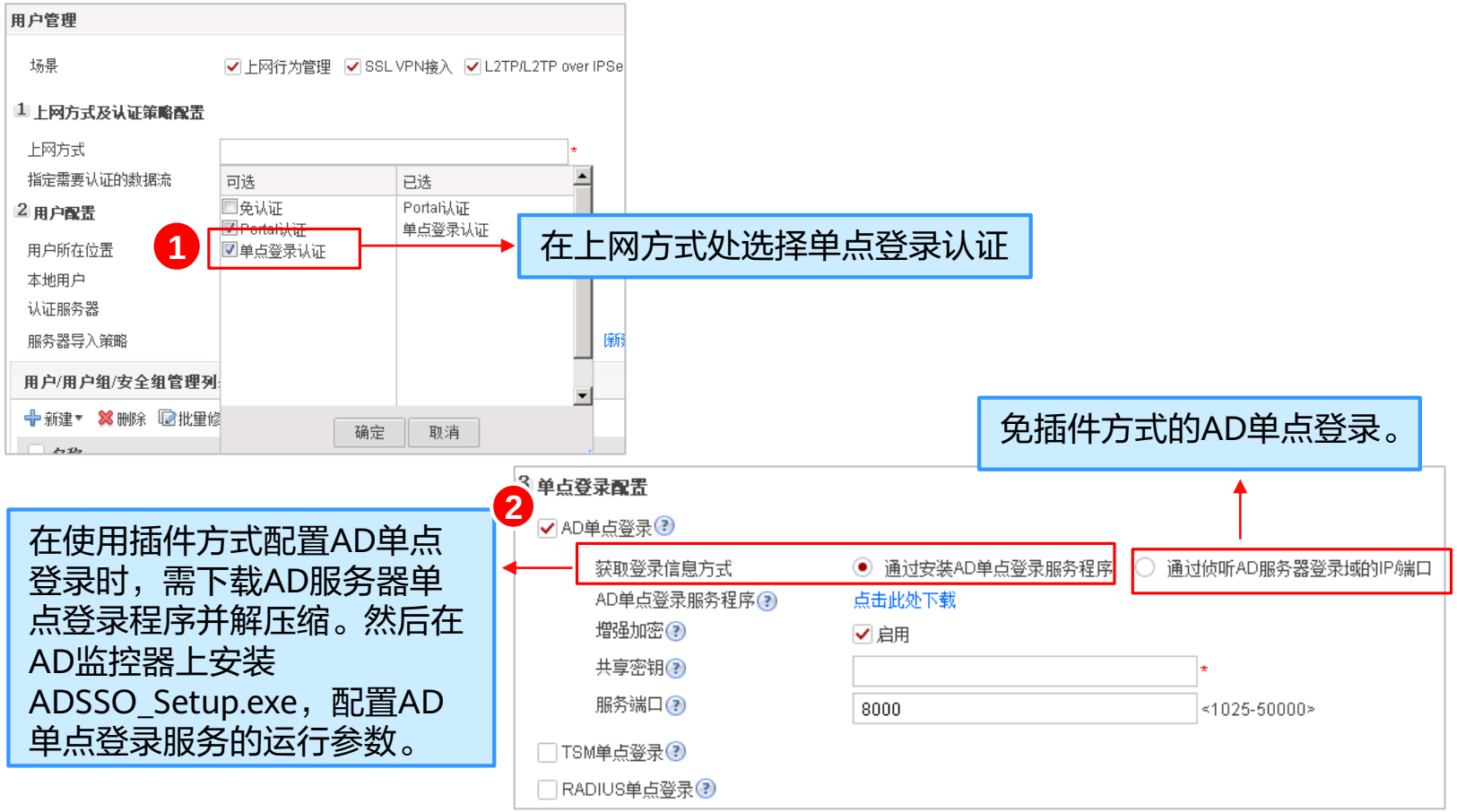
该选项表示用户首次登录认证页面时，必须修改密码。

上网用户使用web重定向推送认证页面时需要配置该部分，认证端口默认使用8887端口。



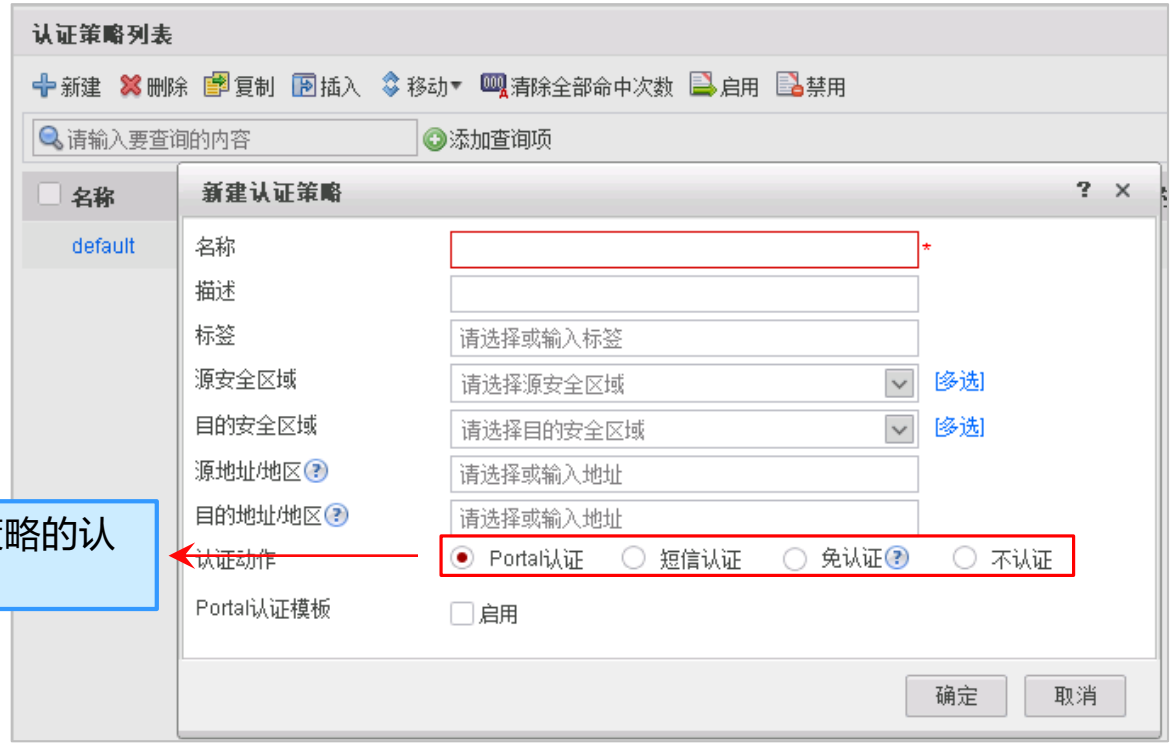
配置认证选项 (单点登录)

- 在“对象> 用户 > default > 上网方式及认证策略配置”，配置单点登录。



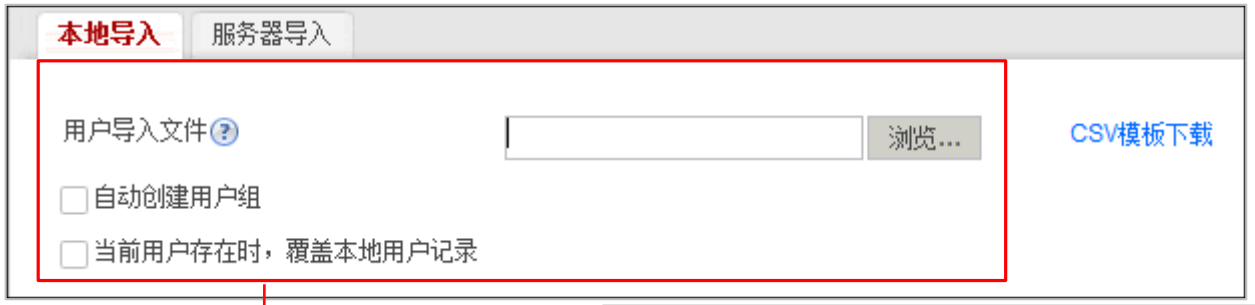
配置认证策略

- 在“对象> 用户 > 认证策略 > 新建”，配置认证策略。



通过本地和服务器导入用户

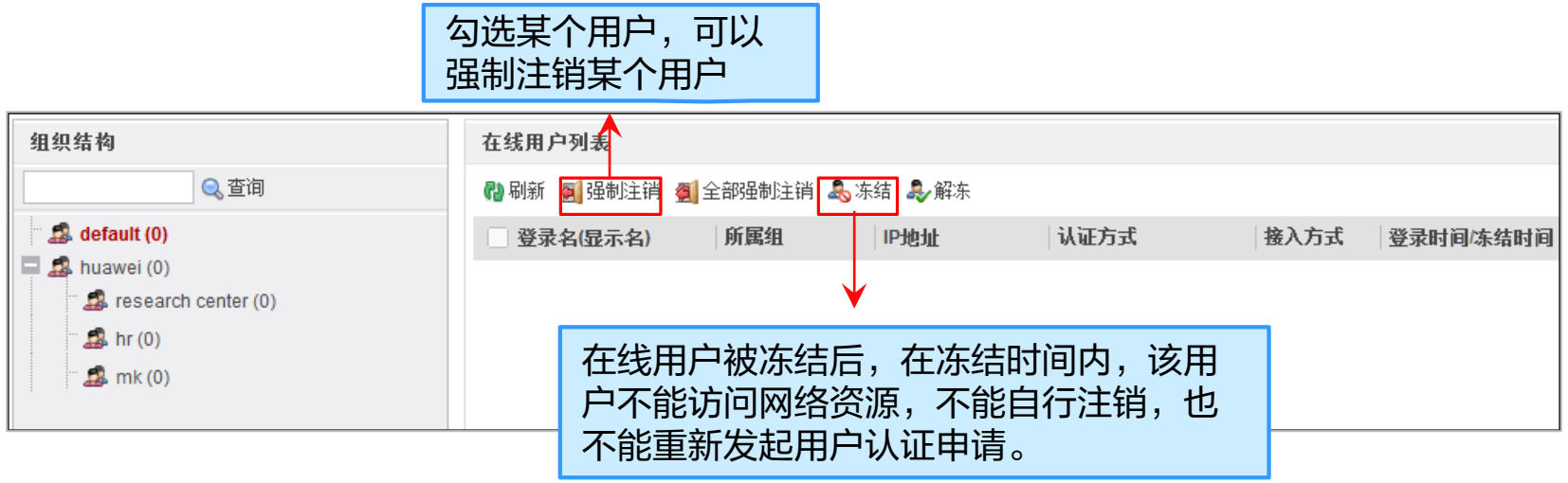
- 选择“对象> 用户 > 用户导入”。
  - 本地导入:本地导入支持将CSV格式文件和数据库dbm文件的用户信息导入到设备本地。
  - 服务器导入:从认证服务器上批量导入用户是指通过服务器导入策略，将认证服务器上用户（组）信息导入到设备上。



下载CSV模板，补充完整数据后，点击浏览，并上传数据。

在线用户管理

- 在“对象> 用户 > 在线用户”，可以对在线用户进行管理。
- 若需要限制某些用户在某段时间内所有上网行为，可以冻结指定的在线用户。
- 若管理员觉察到某些用户不可信，可以强制注销指定的在线用户。



思考题

1. 以下哪个选项不属于AAA（　　）？

A. 认证

B. 授权

C. 计费

D. 管理

目录

病毒简介

- 病毒是一种在人为或非人为的情况下产生的、在用户不知情或未批准下，能自我复制或运行的，计算机**指令**或**程序代码**。

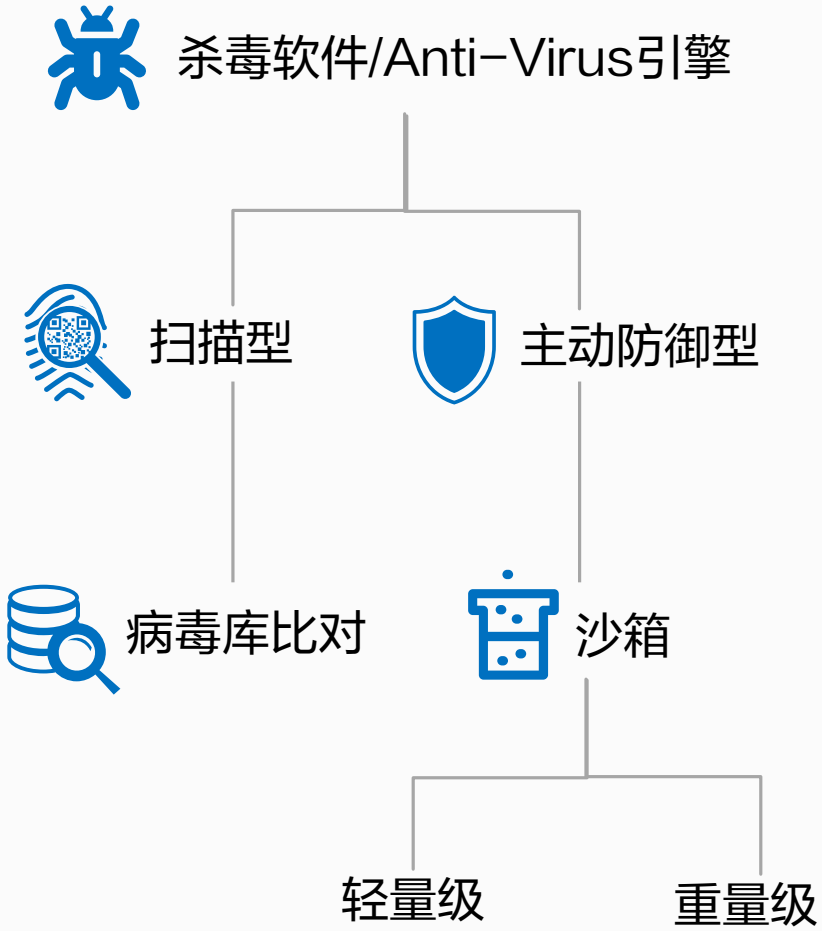
病毒的种类	木马病毒、系统病毒、蠕虫病毒、脚本病毒、后门病毒、恶作剧病毒
传播途径	网络（电子邮件、网页链接、P2P共享）、U盘等

漏洞可辅助传播病毒

利用网站漏洞挂木马病毒

利用程序/系统漏洞传播病毒

病毒防范



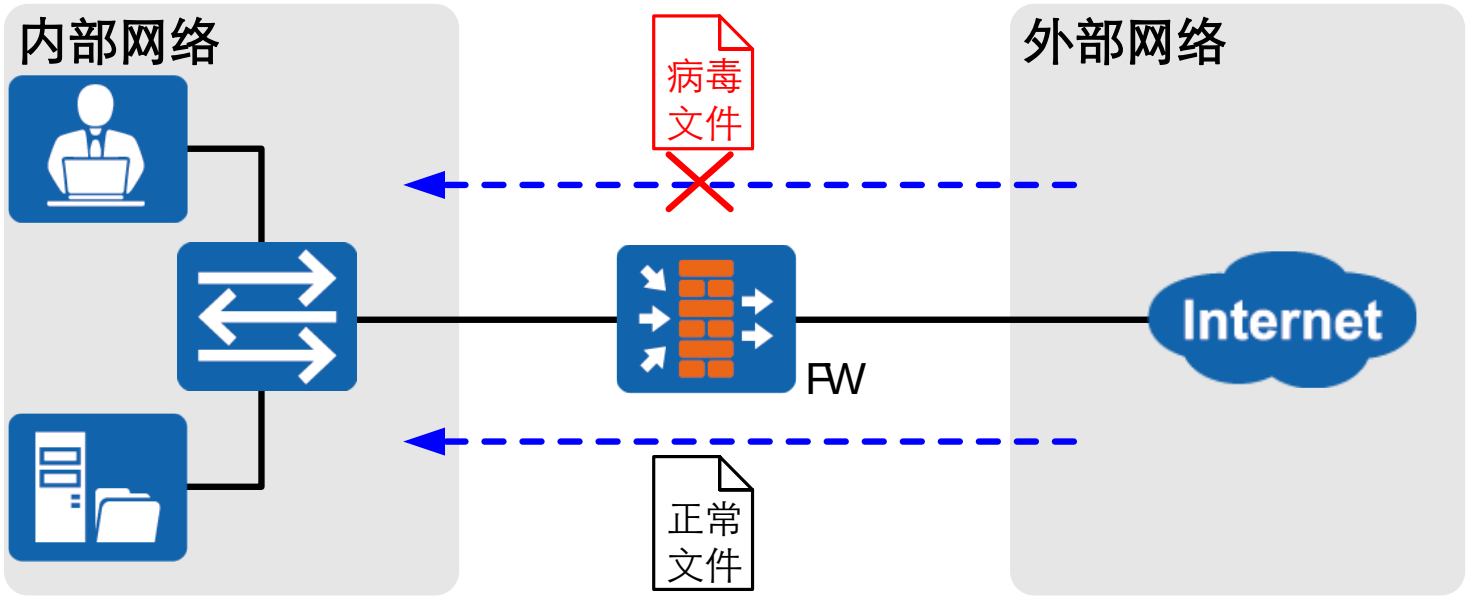
主机侧（服务器/用户主机）

- 安装杀毒软件
- 定期更新系统，安装补丁

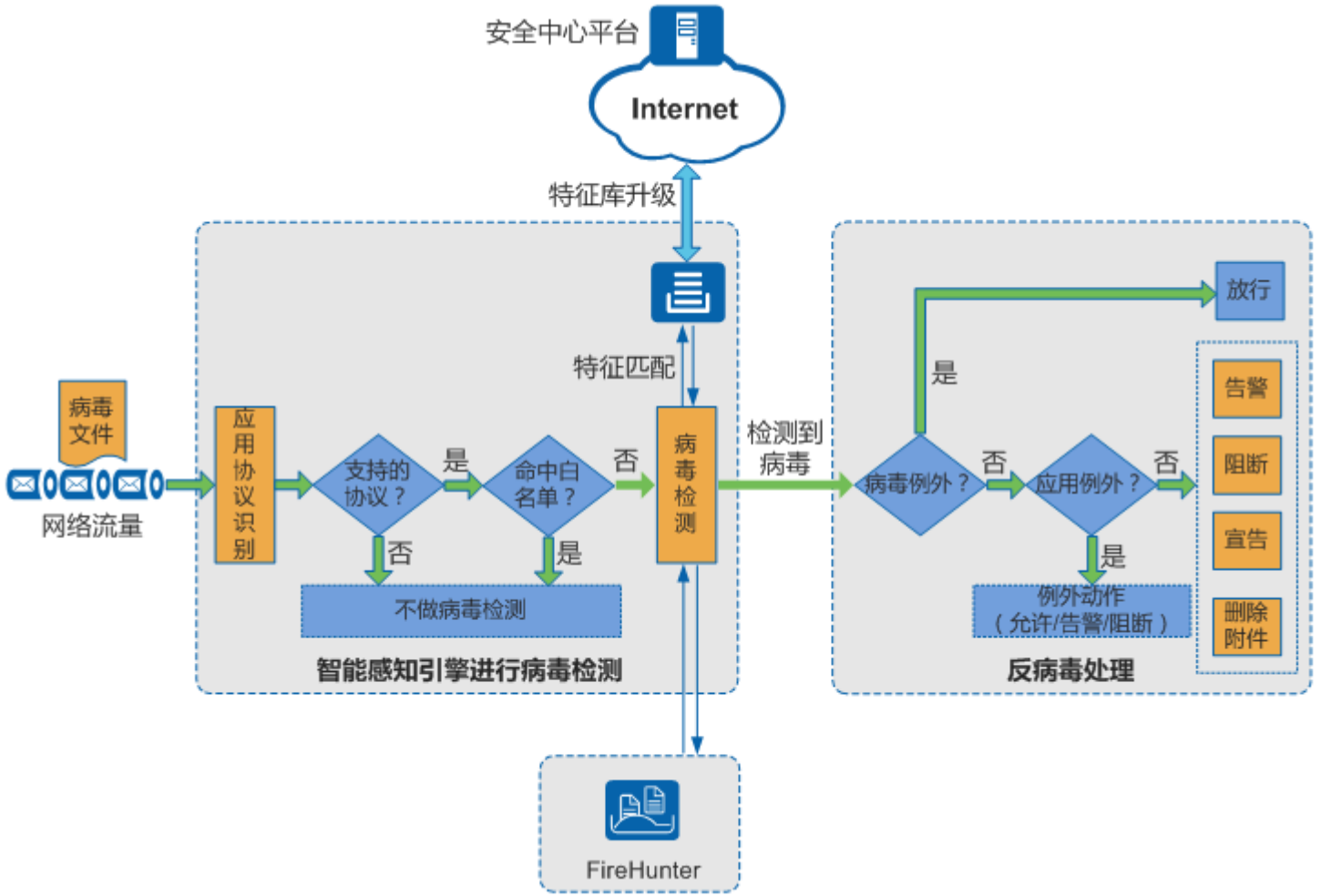
网络侧

- 防火墙
- 防毒墙
- 沙箱
- 业务感知过滤业务

网关防病毒应用场景

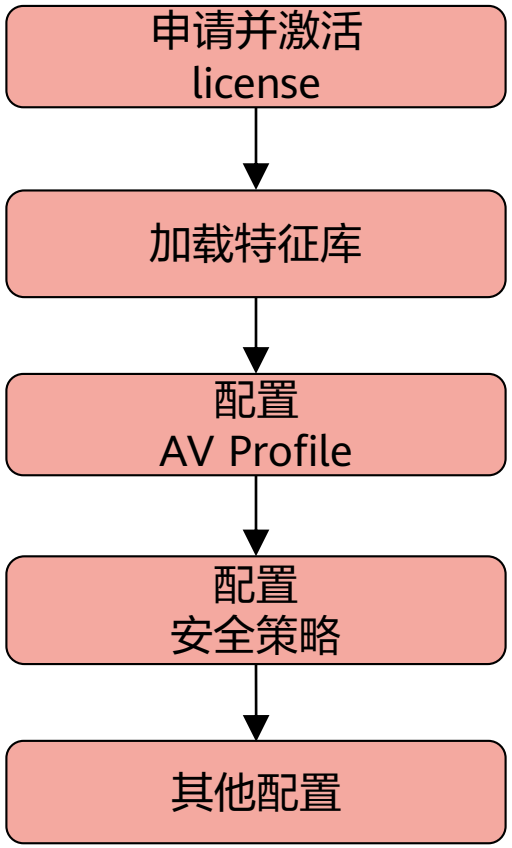


反病毒工作原理



反病毒配置思路

- 反病毒的基本配置思路如下：



激活license操作

- 进入“系统→License管理”，激活反病毒License。

加载AV库

- 加载AV特征库。
  - 通过在线升级方式加载。
  - 通过本地升级方式加载。

配置AV Profile（1/3）

- 进入“对象→安全配置文件→反病毒”，配置AV Profile。
  - 根据需要配置病毒文件攻击取证。
  - 根据需要配置文件信誉检测。
  - 配置各协议响应方式。

配置AV Profile（2/3）

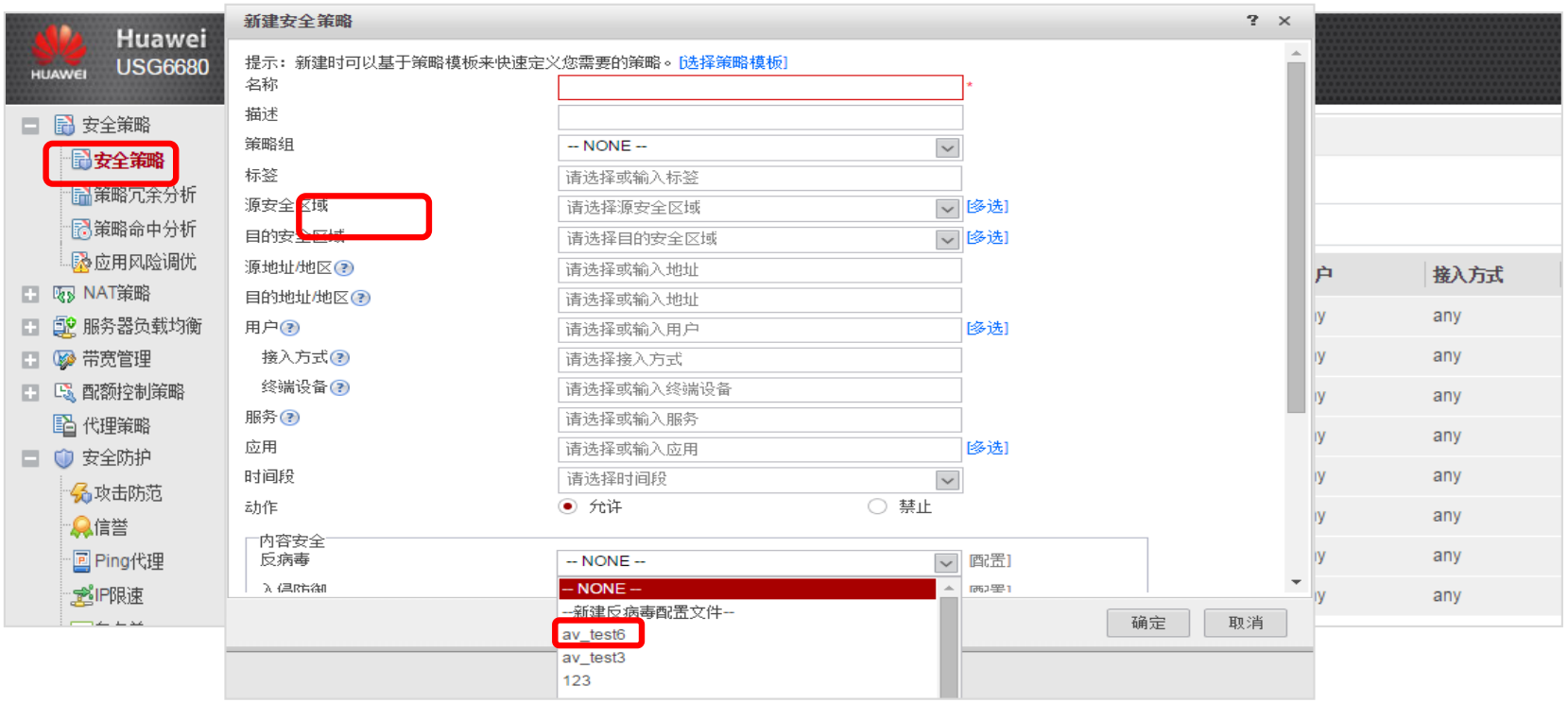
- 如果要为协议中的某个应用配置不同的响应动作，可以在应用例外中完成。
  - 选择特定的应用例外名称，点击添加。
  - 配置响应动作。

配置AV Profile（3/3）

- 如果用户认为某个病毒为误报，可以根据病毒ID配置病毒例外。
  - 进入“监控 > 日志 > 威胁日志”，选择威胁类型为病毒的表项，单击威胁ID对应的值，添加至对应的AV Profile。或者复制威胁ID，手动添加病毒例外。

配置安全策略

- 配置安全策略。
  - 进入“策略 > 安全策略 > 安全策略 > 新建 > 新建安全策略”。
  - 引用反病毒策略。



配置SMTP、POP3和HTTP协议宣告信息

- 进入“系统→推送信息配置”，配置推送信息。
  - 配置SMTP和POP3协议反病毒检测响应方式为宣告时的宣告信息。
  - 配置SMTP和POP3协议反病毒检测响应方式为删除附件时的宣告信息。
  - 配置HTTP协议反病毒检测响应方式为阻断时的宣告信息。

思考题

- 单选题

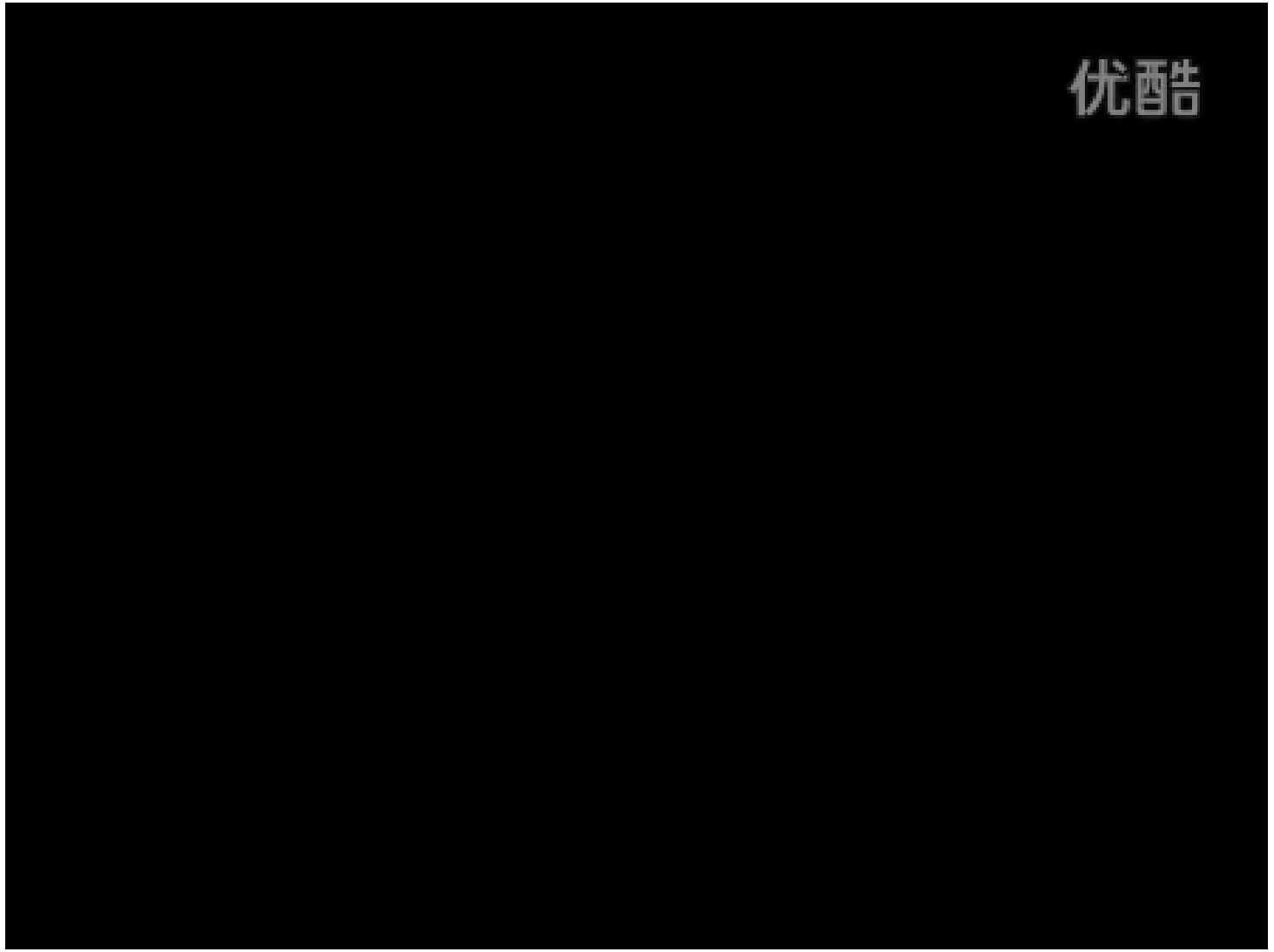
  AV功能不能支持的协议类型是：（　）

  A、HTTP　　B、FTP　　C、SMTP　　D、POP3

目录

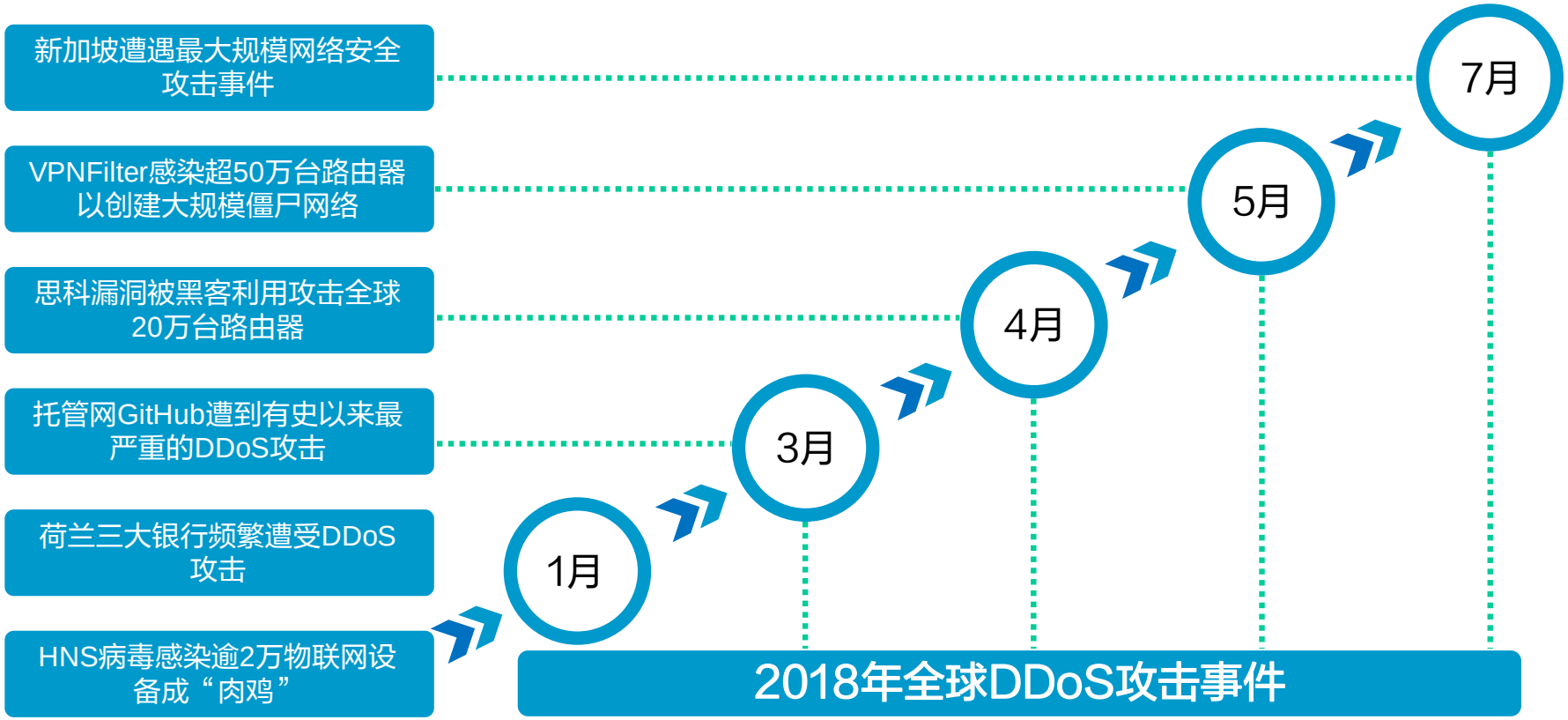
网络攻击典型代表—DDoS攻击

- DDoS攻击往往处于攻击链的最后一步，它利用大流量数据搞瘫服务器，因此DoS攻击叫**拒绝服务攻击**（Denied of Service）。
- 又由于目前DoS攻击的僵尸主机来源广泛，分布在各个网络区域，因此有了DDoS-**分布式拒绝服务攻击**（Distribute Denied of Service）



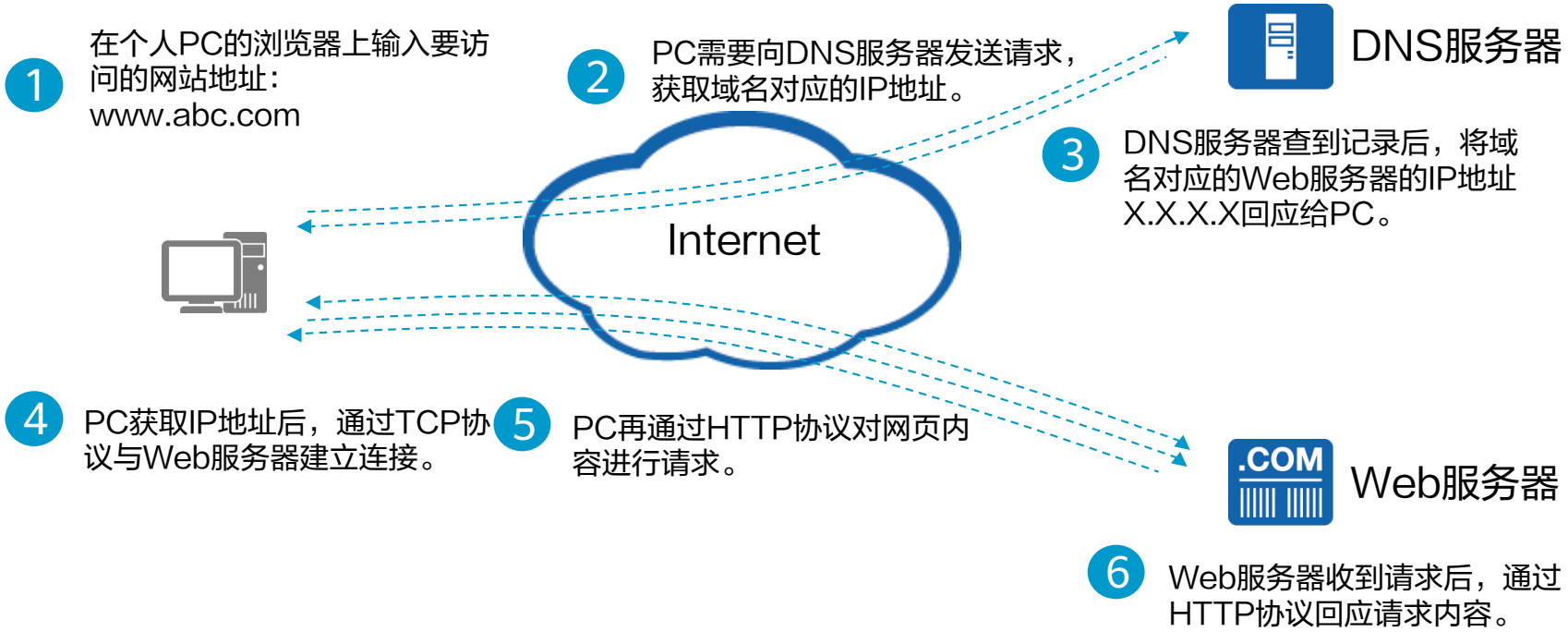
全球DDoS攻击事件

- DDoS在全球的攻击事件越来越频繁，网络安全问题已经从小规模事件上升到国家安全层面，我们先回顾一下2018年爆发的重大DDoS攻击事件。



从Web访问流程分析DDoS攻击

- 当访问某网站的资源时，一次访问的简化过程如下。

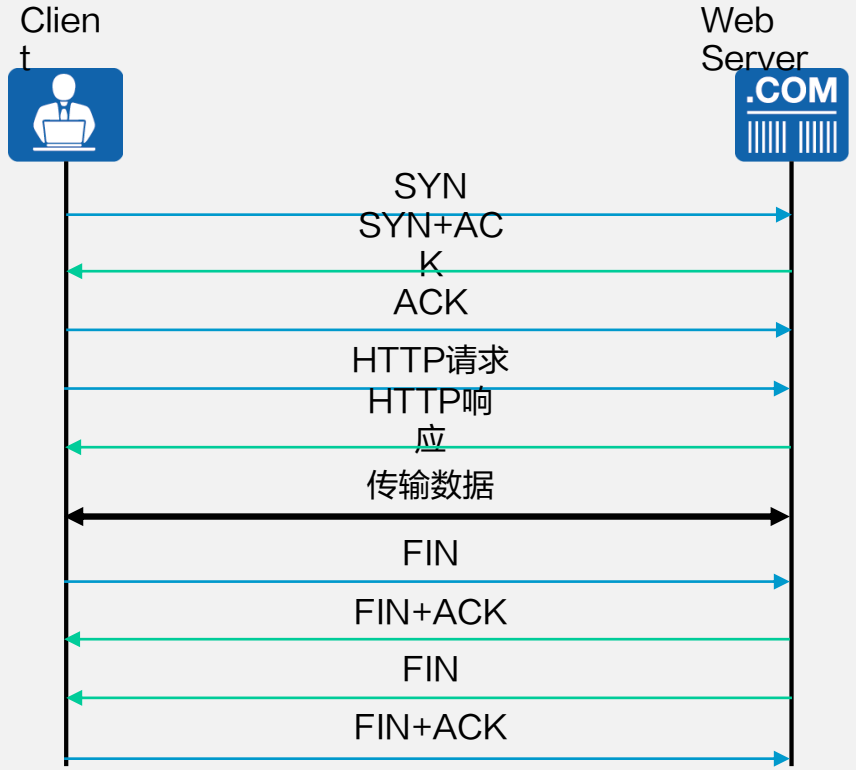


- 可以看出一次Web访问至少涉及了3个协议，DDoS攻击针对Web服务器的攻击就是从该流程入手发起的。

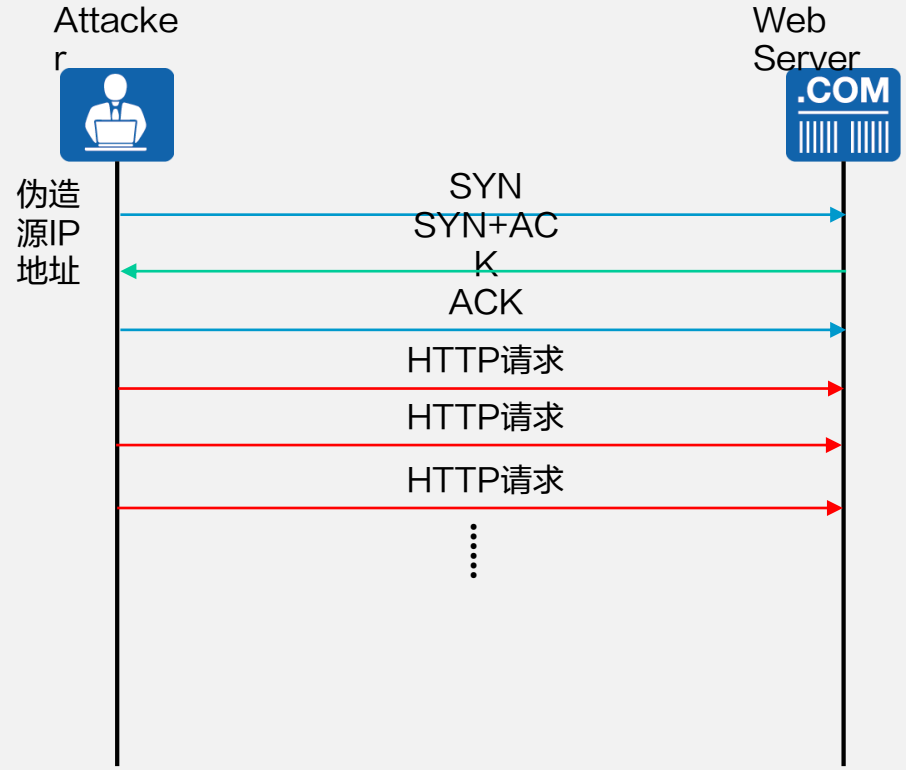
HUAWEI

利用HTTP请求发动HTTP Get Flood攻击

正常HTTP协议工作过程

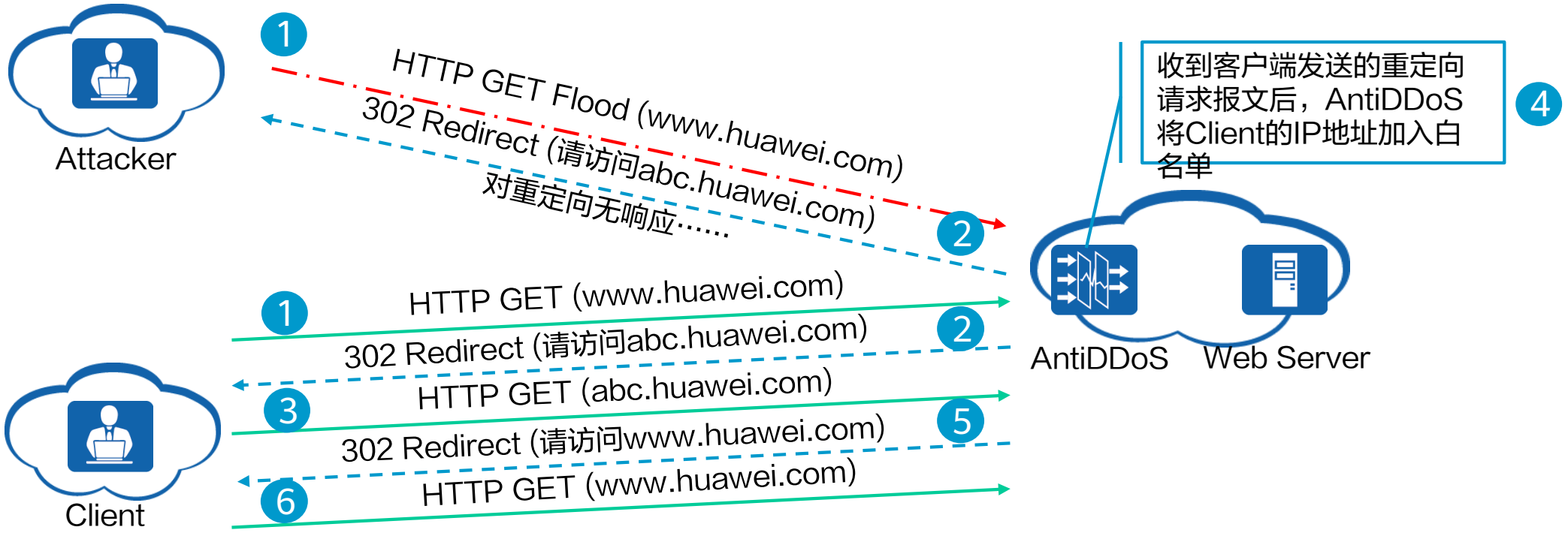


利用HTTP请求发起DDoS攻击



AntiDDoS针对HTTP GET Flood防御原理

- 302重定向认证
  - Anti-DDoS系统代替服务器向客户端响应302状态码（针对GET请求方法的重定向），告知客户端需要重定向到新的URL，以此来验证客户端的真实性。



思考题

1. (单选)某电子商城购物节活动，导致网站响应速度慢，这是不是一种DDoS攻击?

A. 是

B. 否

本章总结

- 防火墙概述
- 用户认证技术
- 反病毒技术
- DDoS防御原理


谢 谢
www.huawei.com