防火墙介绍

www.huawei.com

HUAWEI

前言

- 在数据通信过程中，由于网络中的不安全因素将会导致信息泄密、信息不完整，信息不可用等问题，因此在部署网络时需要用到防火墙设备。
- 本章主要介绍华为防火墙的发展历史、特点、典型组网方式、应用场景和技术指标。

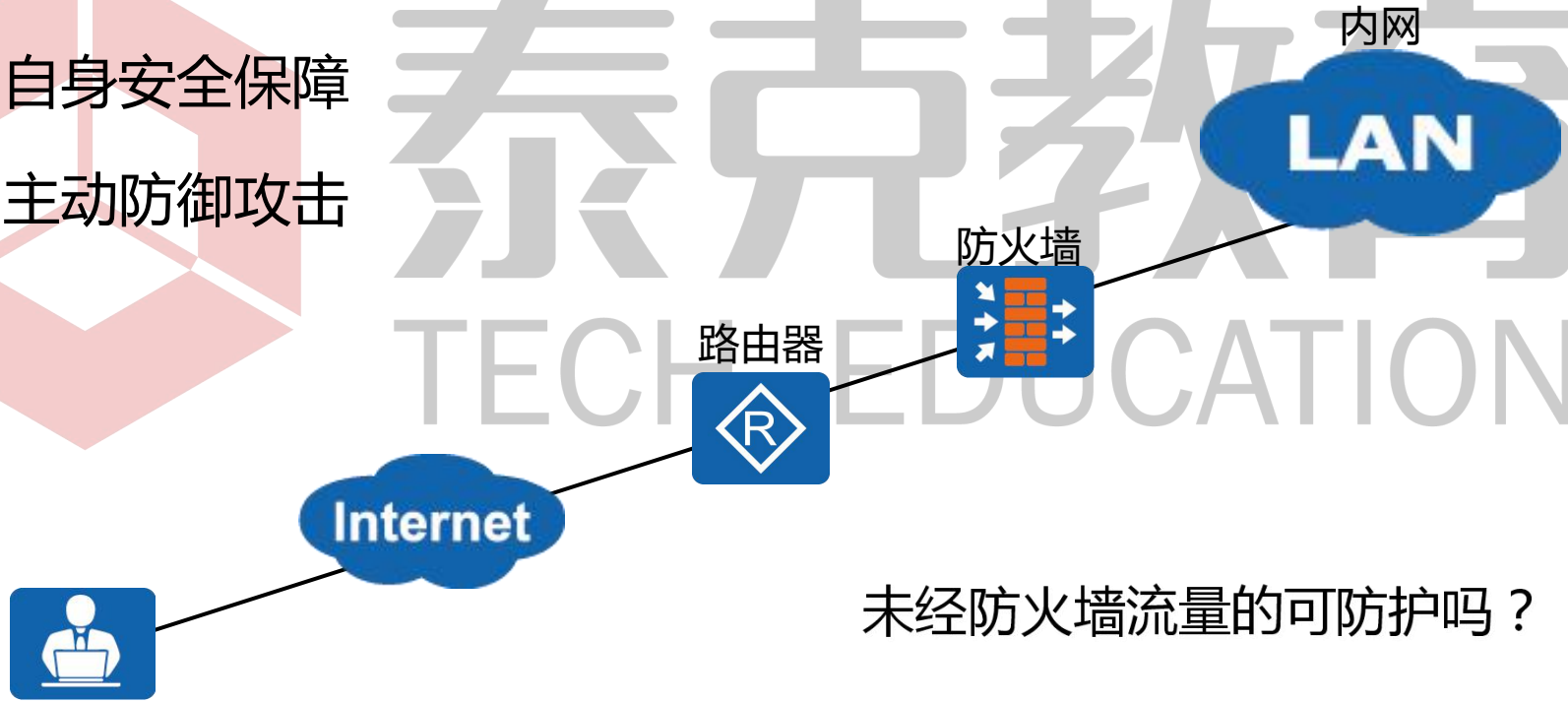
目标

- 学完本课程后，您将能够:
  - 了解防火墙基本概念
  - 理解防火墙安全策略
  - 掌握防火墙安全策略配置

目录

防火墙特征

- 逻辑区域过滤器
- 隐藏内网网络结构
- 自身安全保障
- 主动防御攻击

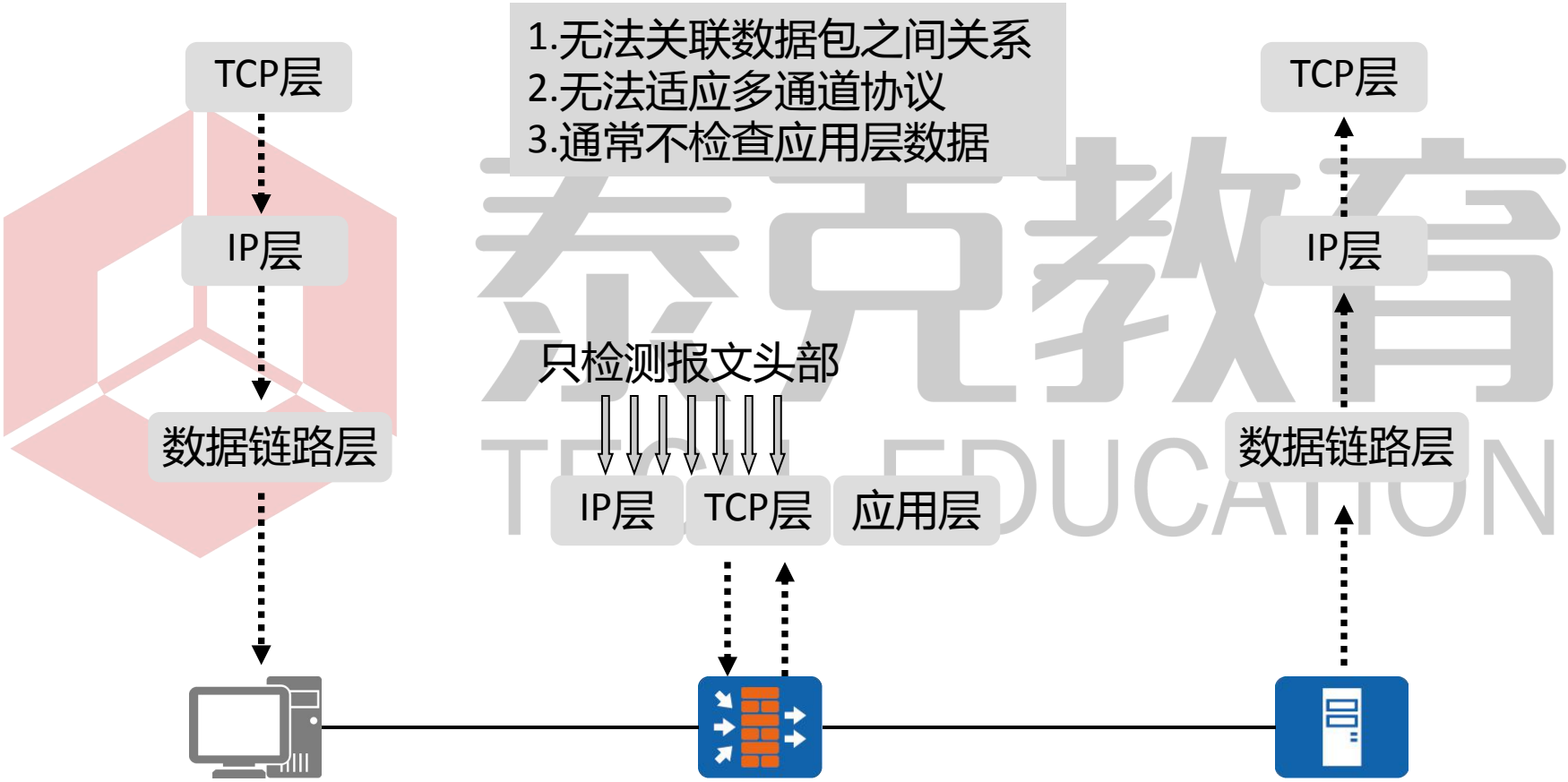


未经防火墙流量的可防护吗？

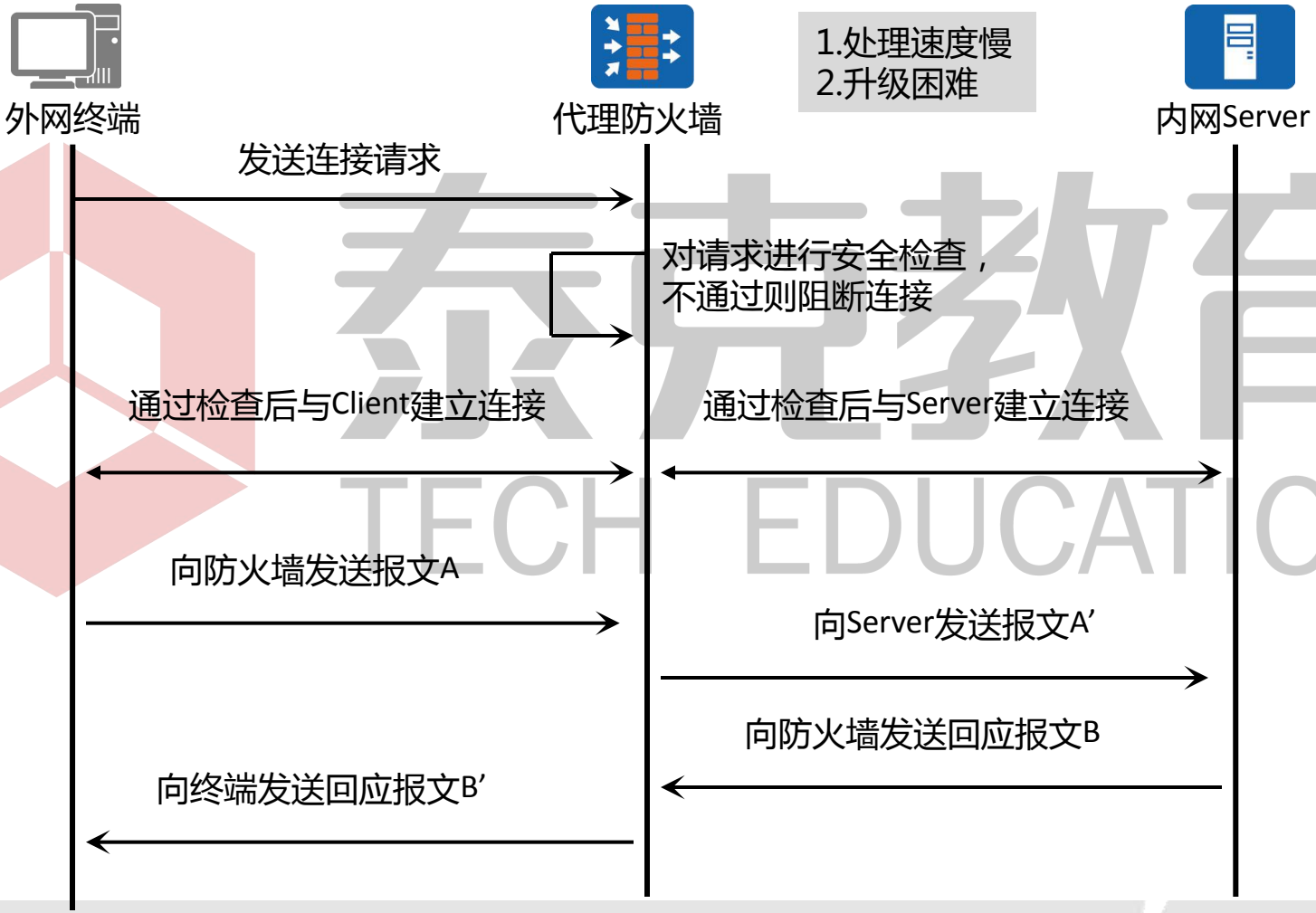
防火墙分类

- 按照访问控制方式分为：
  - 包过滤防火墙
  - 代理防火墙
  - 状态检测防火墙

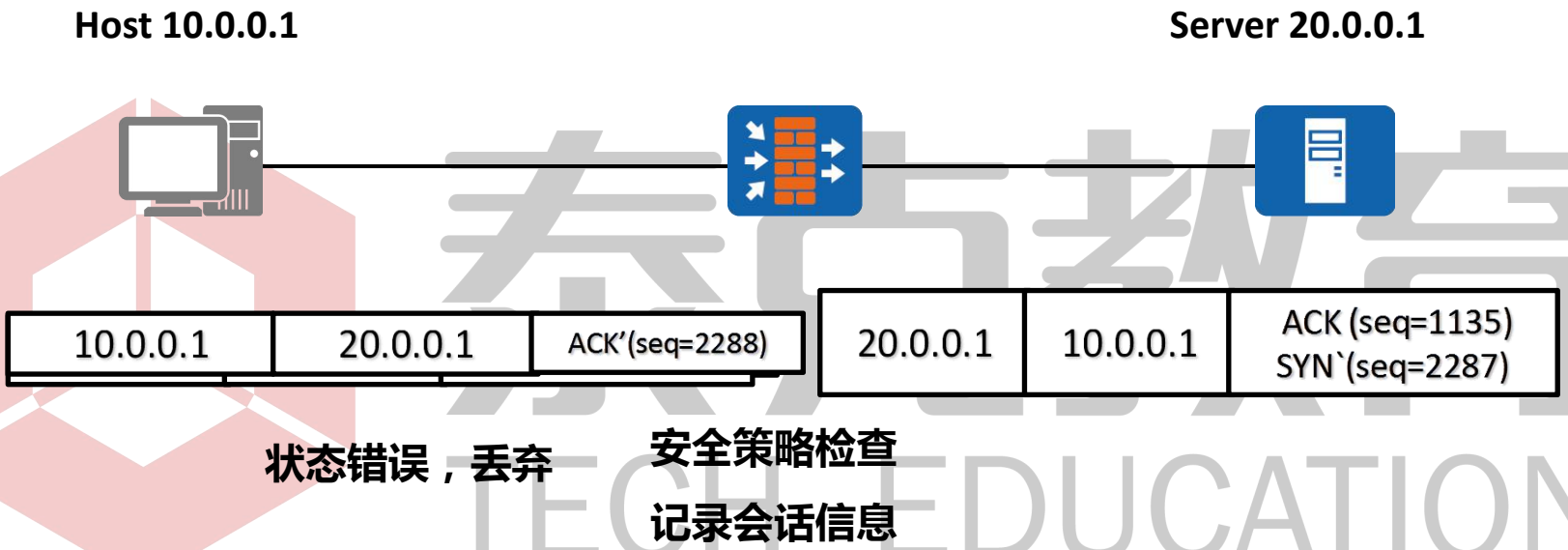
防火墙分类 – 包过滤防火墙



防火墙分类 – 代理防火墙

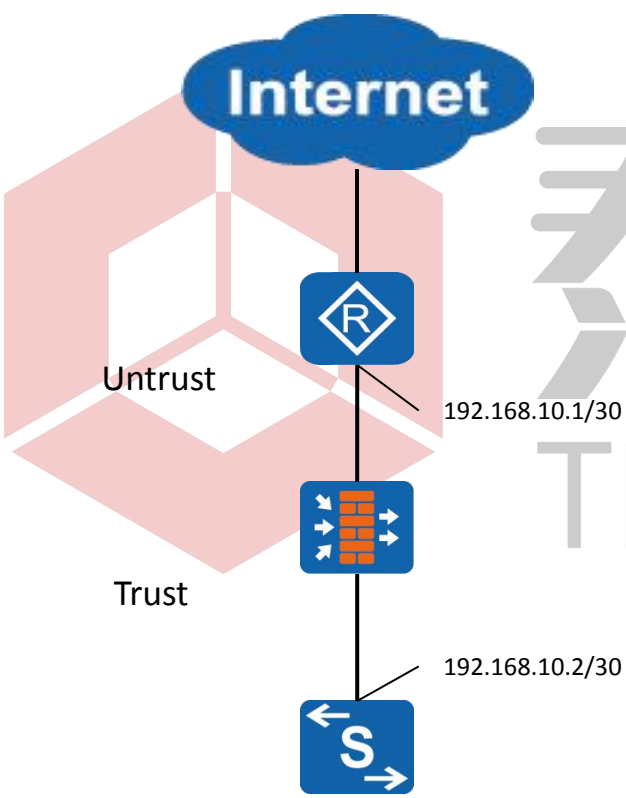


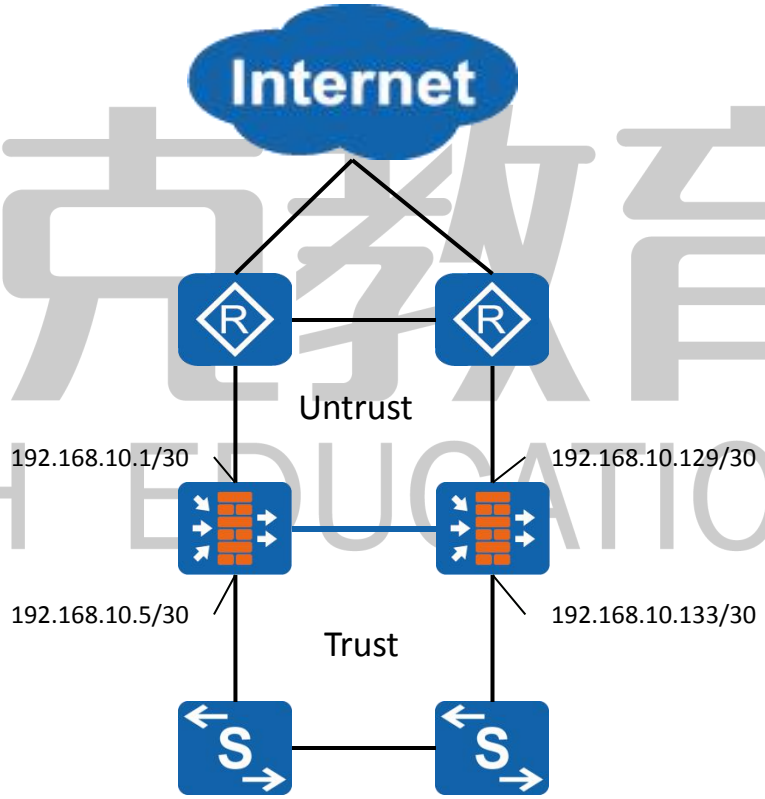
防火墙分类 – 状态检测防火墙



1.处理后续包速度快
2.安全性高

防火墙组网方式

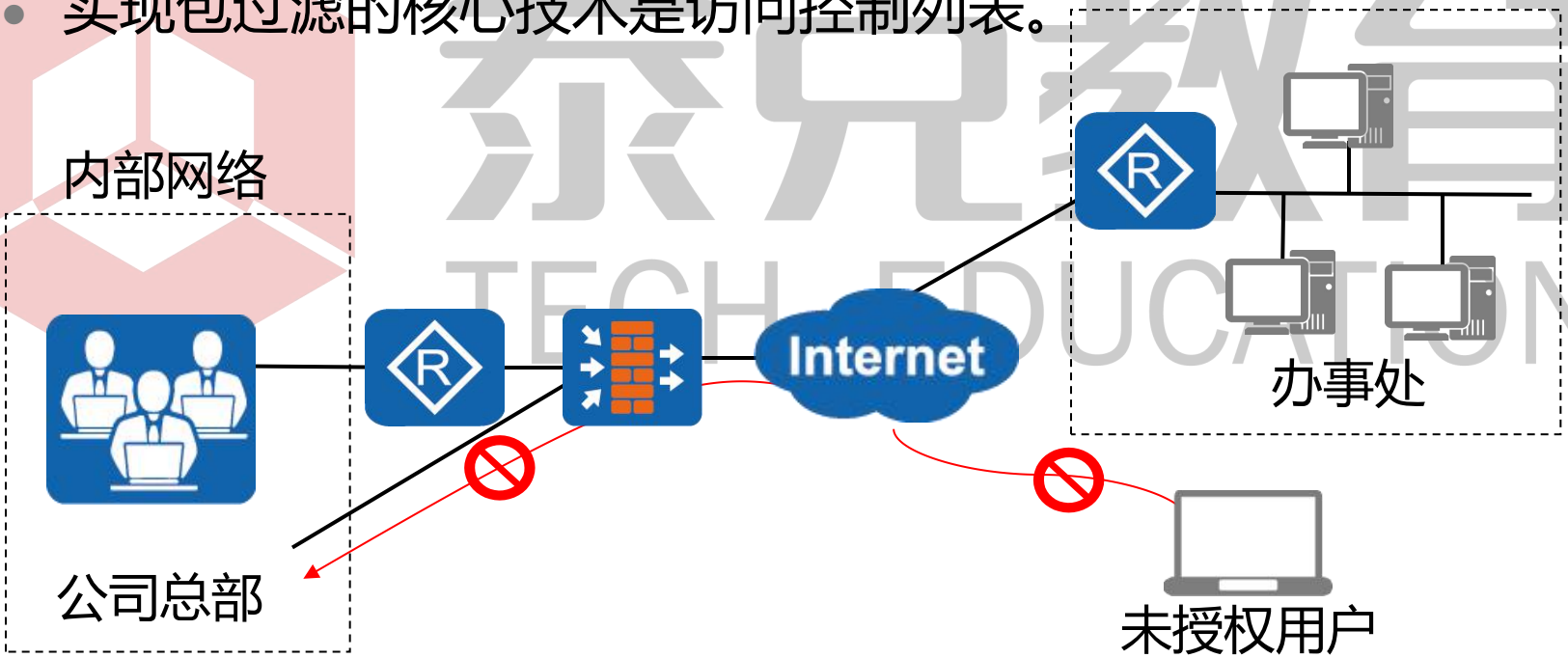




目录

包过滤技术

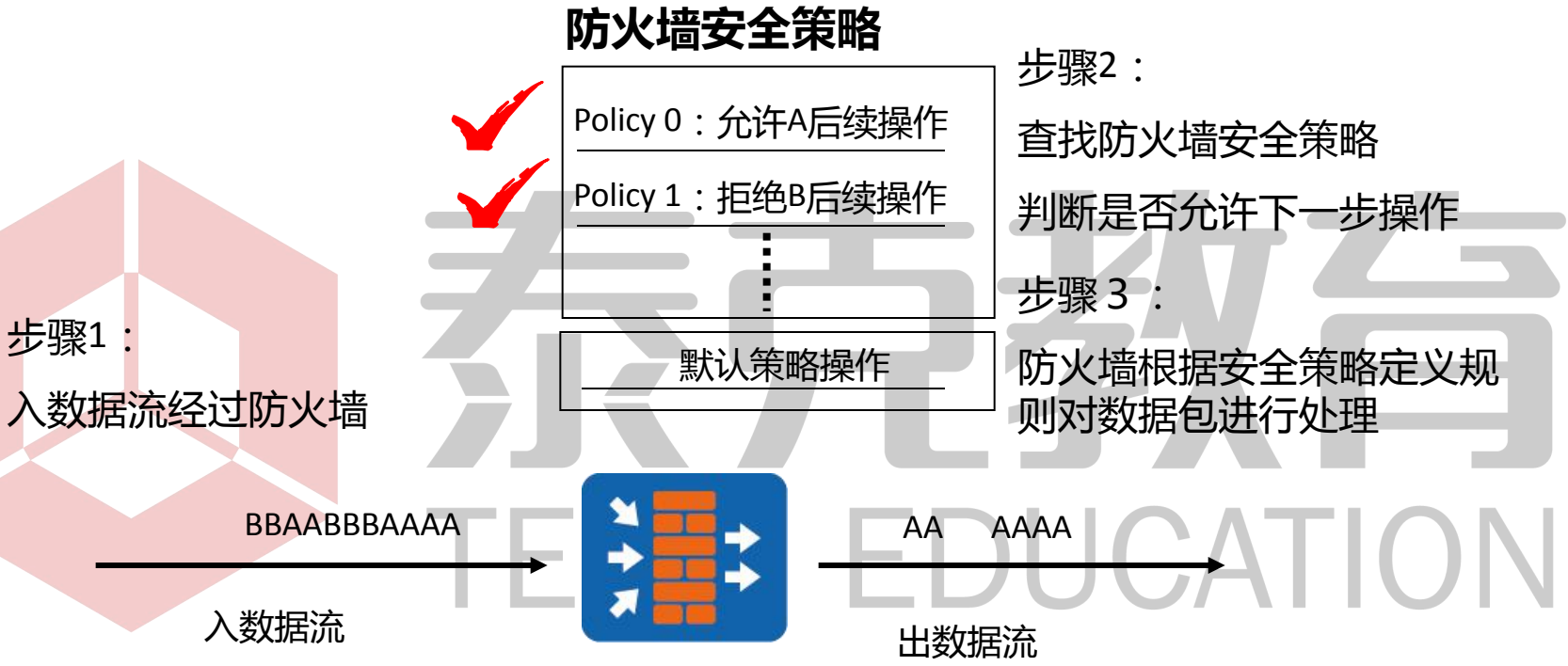
- 对需要转发的数据包，先获取包头信息，然后和设定的规则进行比较，根据比较的结果对数据包进行转发或者丢弃。
- 实现包过滤的核心技术是访问控制列表。



防火墙安全策略

- 定义
  - 安全策略是按一定规则控制设备对流量转发以及对流量进行内容安全一体化检测的策略。
  - 规则的本质是包过滤。
- 主要应用
  - 对跨防火墙的网络互访进行控制。
  - 对设备本身的访问进行控制。

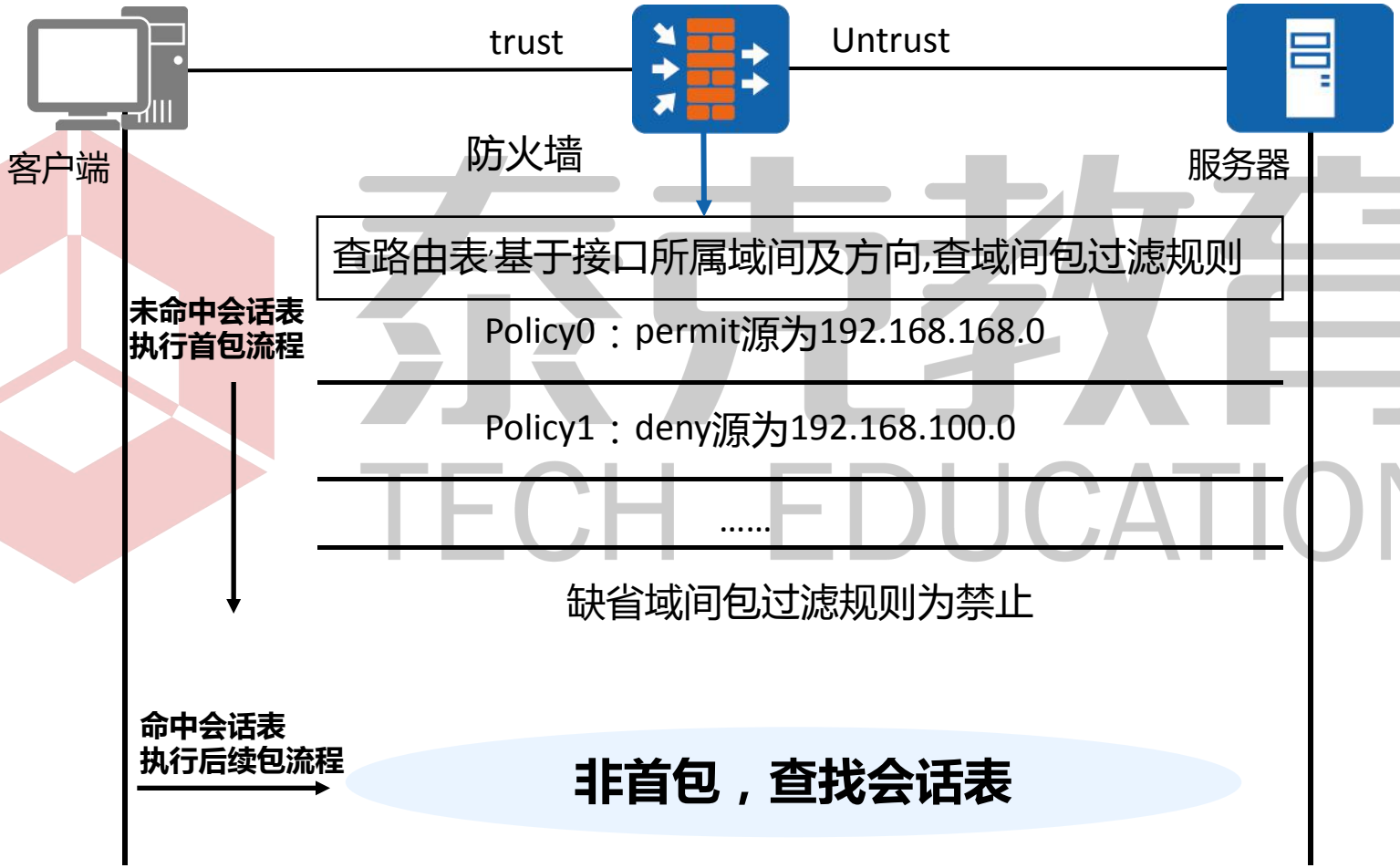
防火墙安全策略的原理



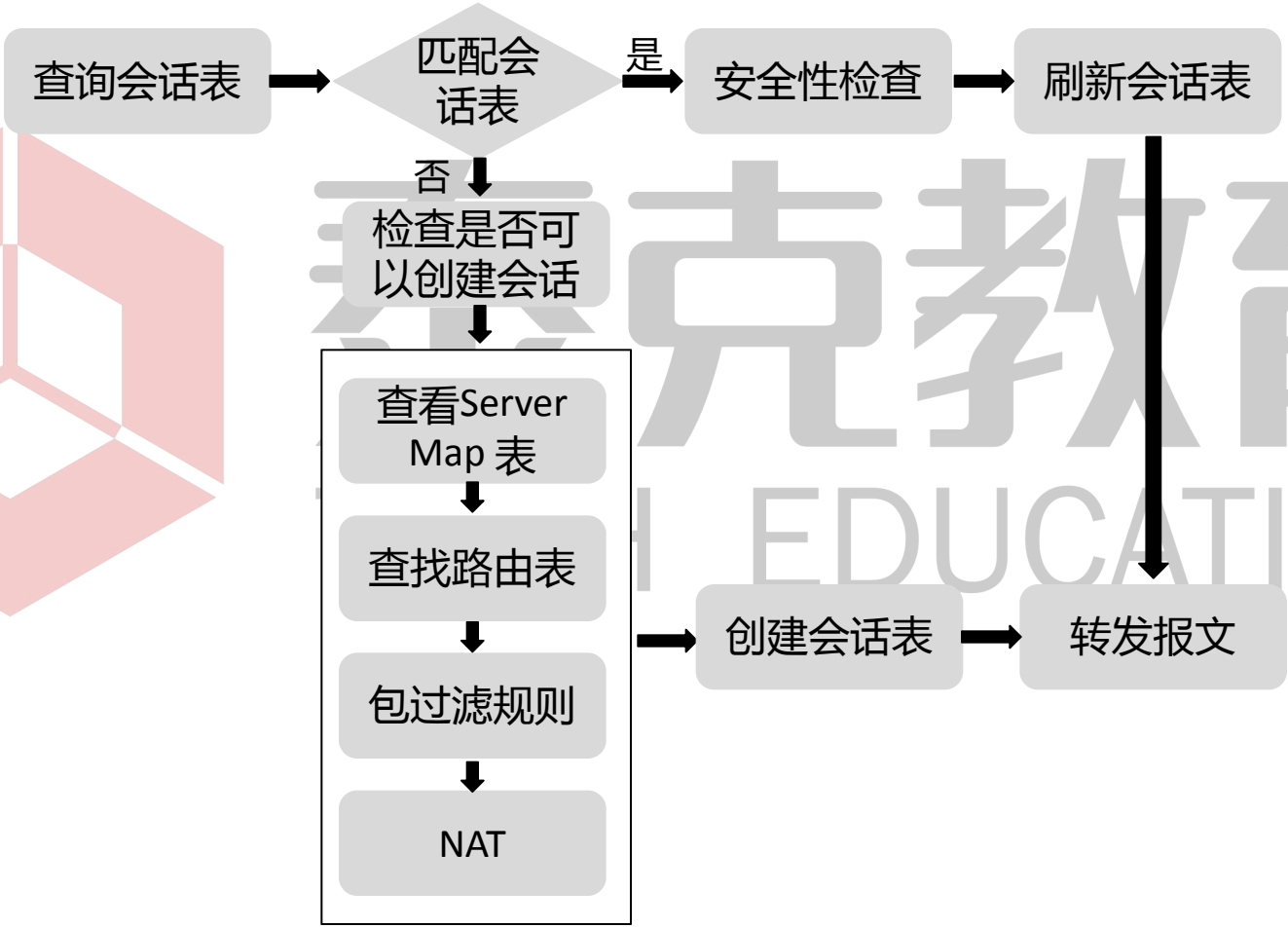
- 防火墙安全策略作用：

根据定义的规则对经过防火墙的流量进行筛选，并根据关键字确定筛选出的流量如何进行下一步操作。

防火墙域间转发

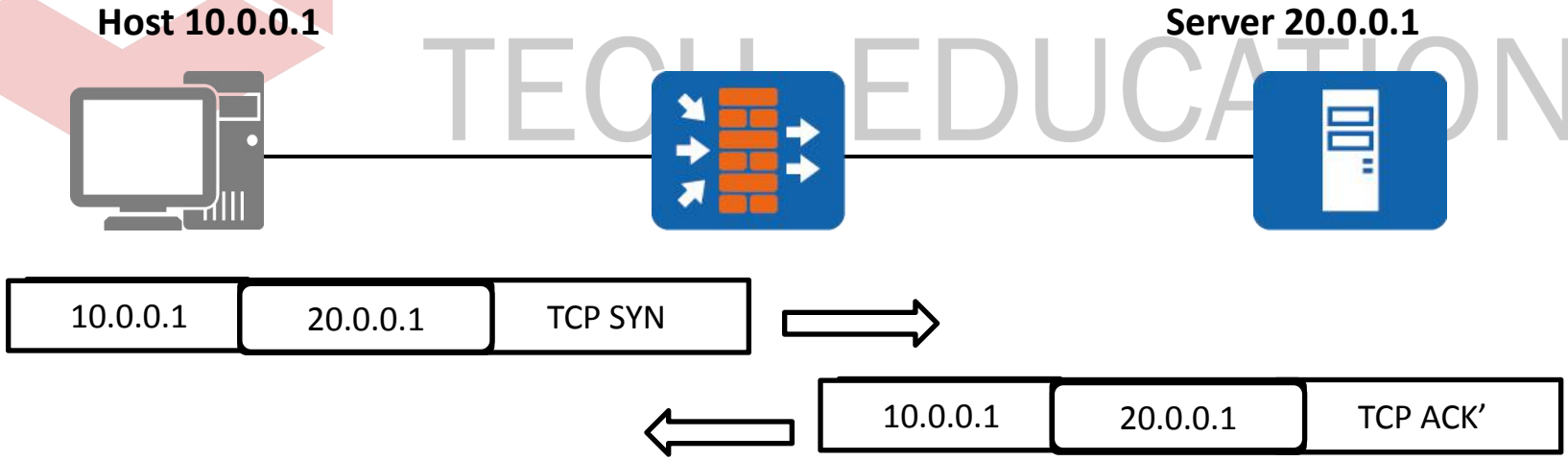


查询和创建会话

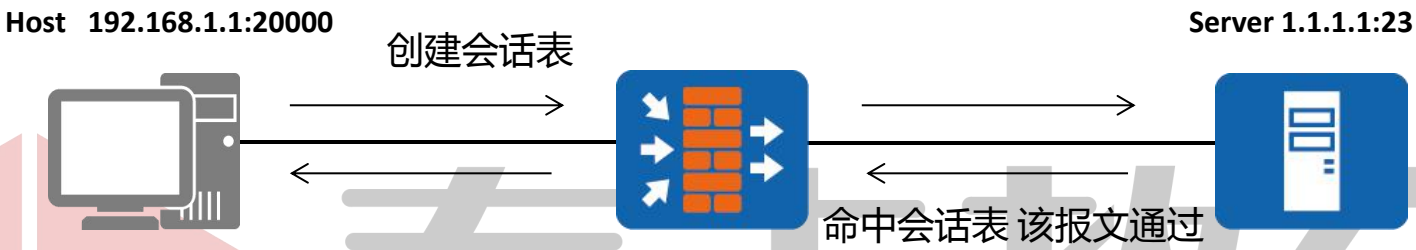


状态检测机制

- 状态检测机制开启状态下，只有首包通过设备才能建立会话表项，后续包直接匹配会话表项进行转发。
- 状态检测机制关闭状态下，即使首包没有经过设备，后续包只要通过设备也可以生成会话表项。



会话表项



Client→ Server

源IP地址	源端口	目的IP地址	目的端口	协议	用户	应用
192.168.1.1	20000	1.1.1.1	23	TCP	abc	Telnet

Server→ Client

源IP地址	源端口	目的IP地址	目的端口	协议	用户	应用
1.1.1.1	23	192.168.1.1	20000	TCP	abc	Telnet

Session: TCP 192.168.1.1:20000 → 1.1.1.1:23

查看会话表信息

- 显示会话表简要信息 display firewall session table

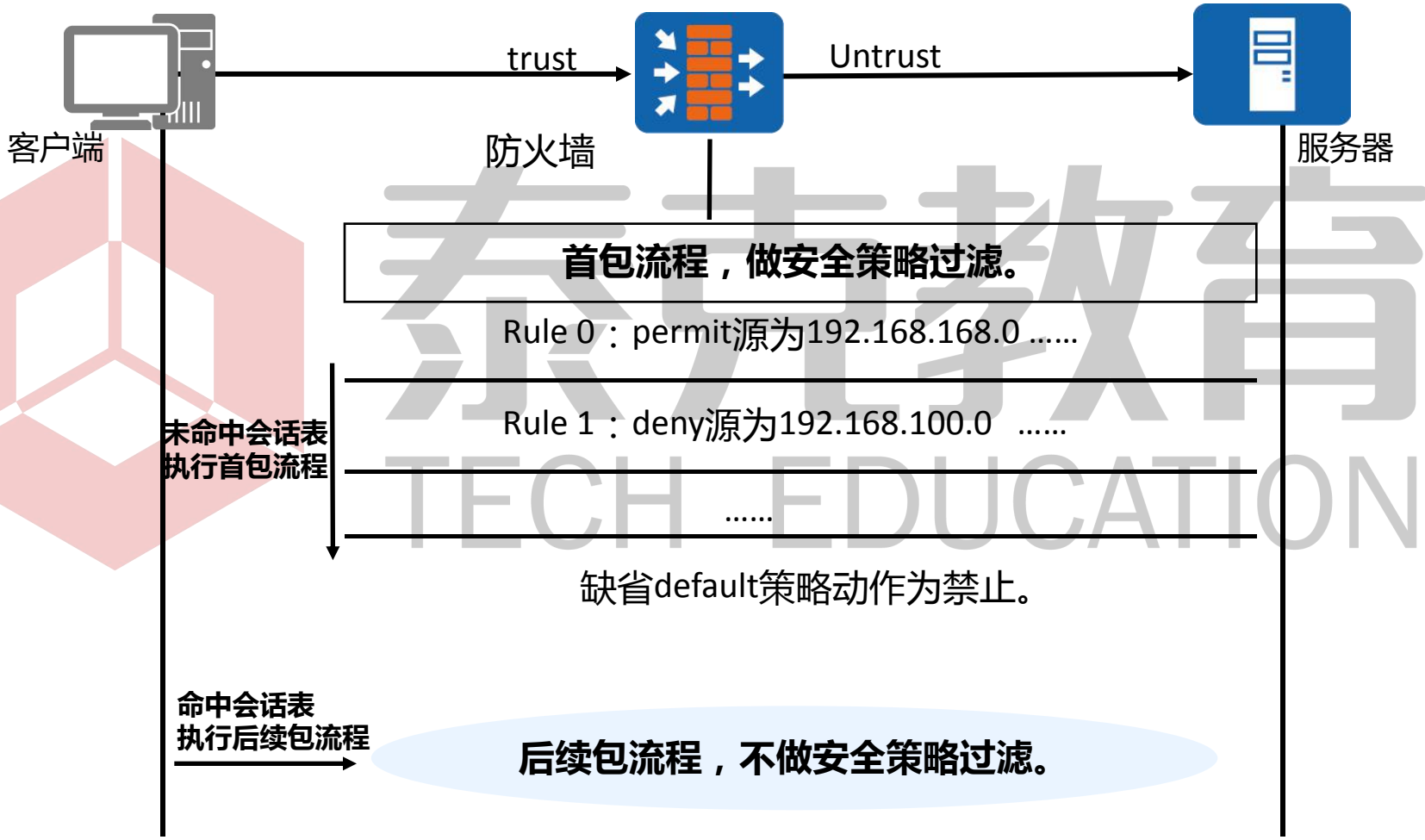
```
<sysname> display firewall session table
Current Total Sessions : 2
   telnet VPN:public --> public 192.168.3.1:2855-->192.168.3.2:23
   http VPN:public --> public 192.168.3.8:2559-->192.168.3.200:80
```

- 显示会话表详细信息 display firewall session table verbose

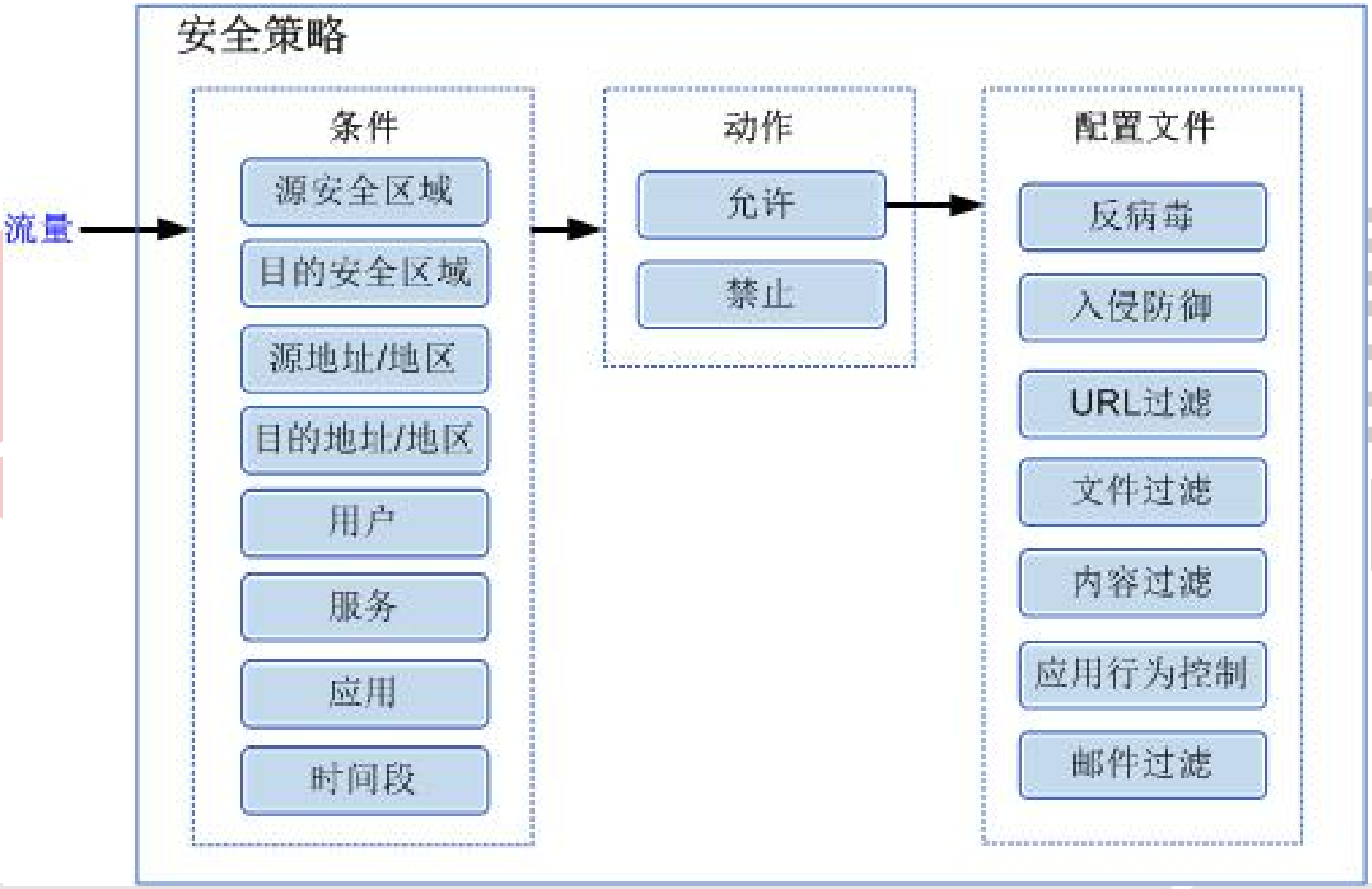
```
<sysname> display firewall session table verbose
Current Total Sessions : 1
   http VPN:public --> public ID: a48f3648905d02c0553591da1
   Zone: trust--> local TTL: 00:20:00 Left: 00:19:56
   Output-interface: InLoopBack0 NextHop: 127.0.0.1 MAC: 00-00-00-
00-00-00
   <--packets:3073 bytes:3251431 -->packets:2881 bytes:705651
   128.18.196.4:1864-->128.18.196.251:80 PolicyName: test
```

目录

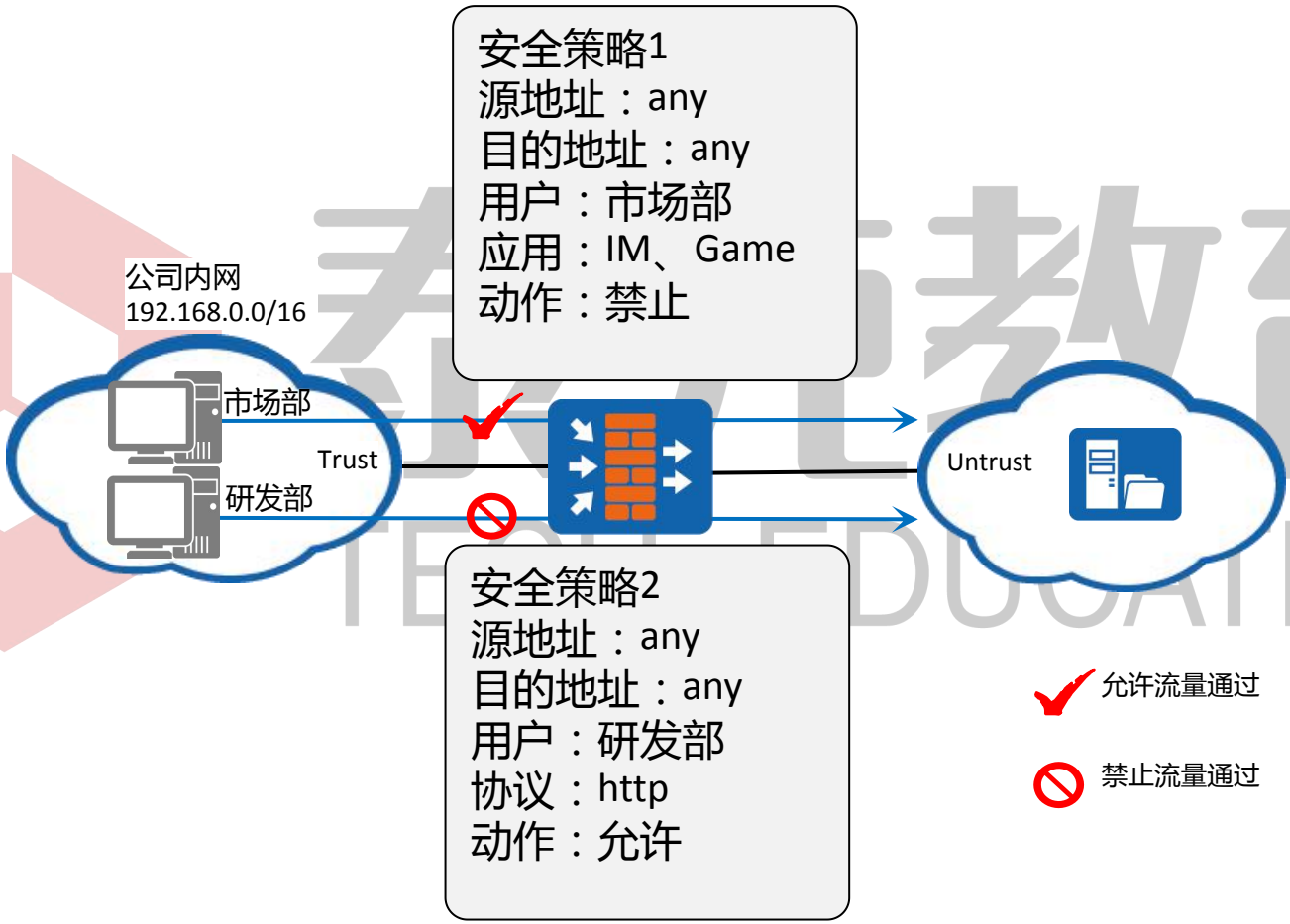
安全策略的匹配原则



安全策略匹配流程

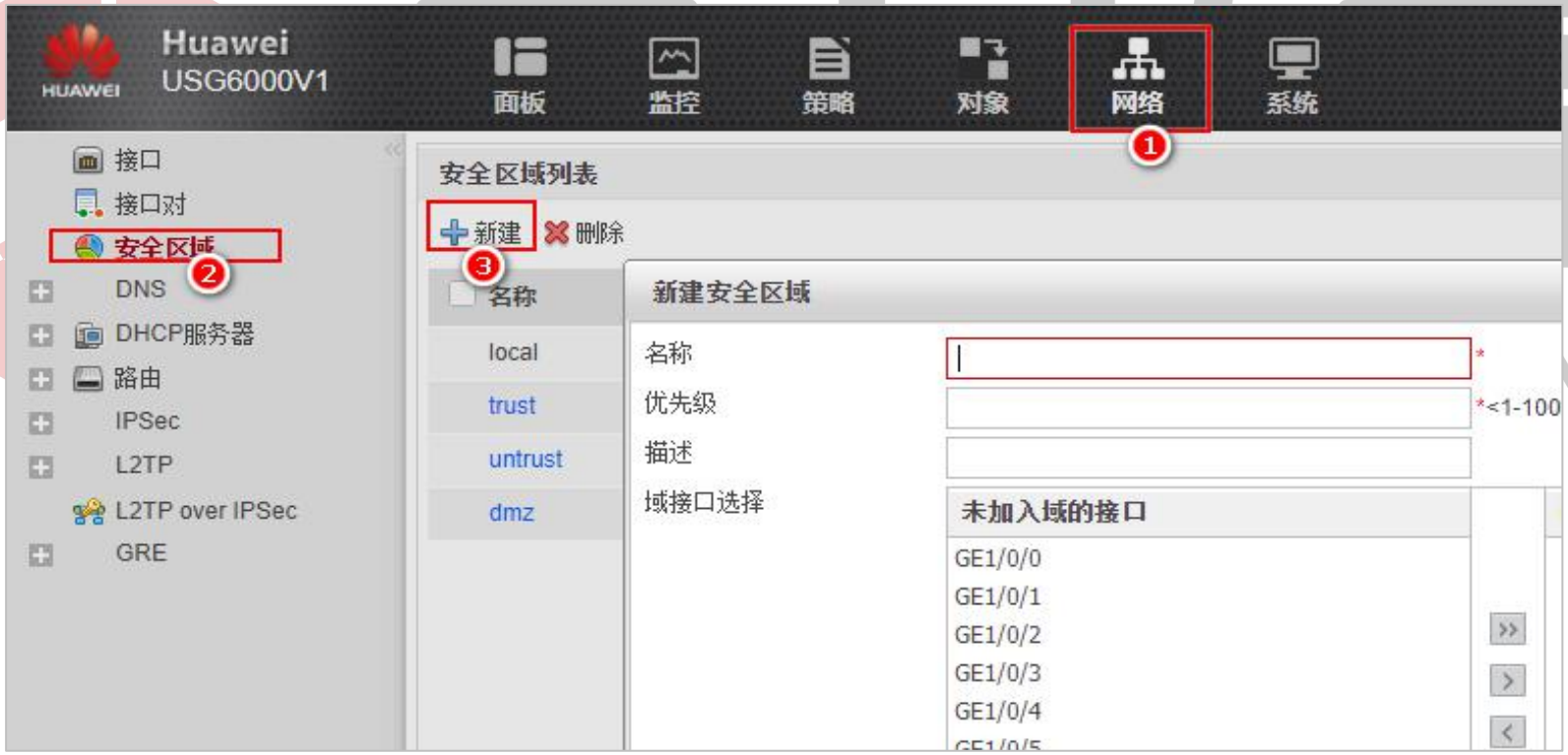


安全策略应用



配置安全区域（WEB）

- 系统缺省已经创建了四个安全区域。如果用户还需要划分更多的安全等级，可以自行创建新的安全区域并定义其安全级别。

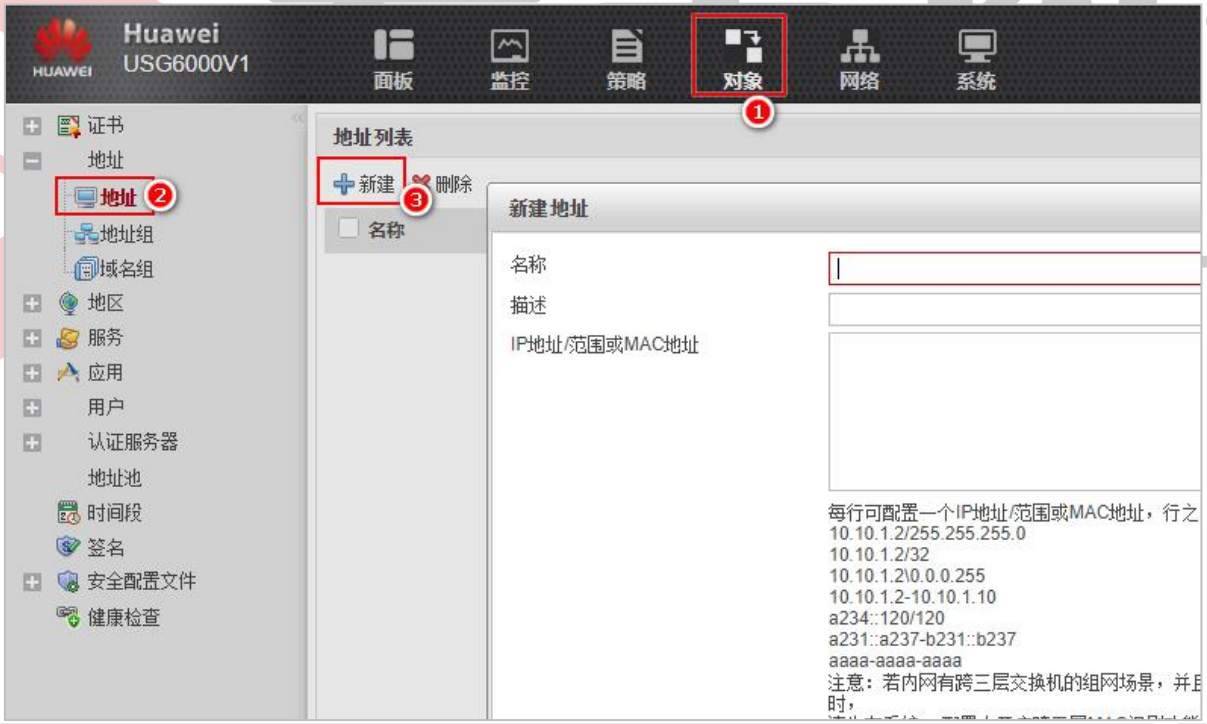


配置安全策略（WEB）

- 安全策略主要包含的配置内容:
  - 策略匹配条件：源安全域，目的安全域，源地址，目的地址，用户，服务，应用，时间段。
  - 策略动作：允许，禁止。
  - 内容安全Profile（可选）：反病毒，入侵防御，URL过滤，文件过滤，内容过滤，应用行为控制，邮件过滤。

配置地址和地址组（WEB）

- 地址是IPv4/IPv6地址或MAC地址的集合，地址组是地址的集合。
- 地址包含一个或若干个IPv4/IPv6地址或MAC地址，它类似于一个基础组件，只需定义一次，就可以被各种策略（例如安全策略、NAT策略）多次引用。



配置地区和地区组（WEB）

- 地区是以地区为单位的IP地址对象，每个地区是当前地区的公网IP地址集合。
- 为方便扩展和复用，设备还支持配置地区组供策略引用。地区组中可以包含多个地区、嵌套的地区组，配置灵活。

配置服务和服务组（WEB）

- 服务是通过协议类型和端口号来确定的应用协议类型，服务组是服务和服务组的集合。
- 预定义服务：指系统缺省已经存在、可以直接选择的服务类型。
- 自定义服务：通过指定协议类型（例如TCP、UDP或ICMP）和端口号等信息来定义的一些应用协议类型。

配置应用和应用组（WEB）

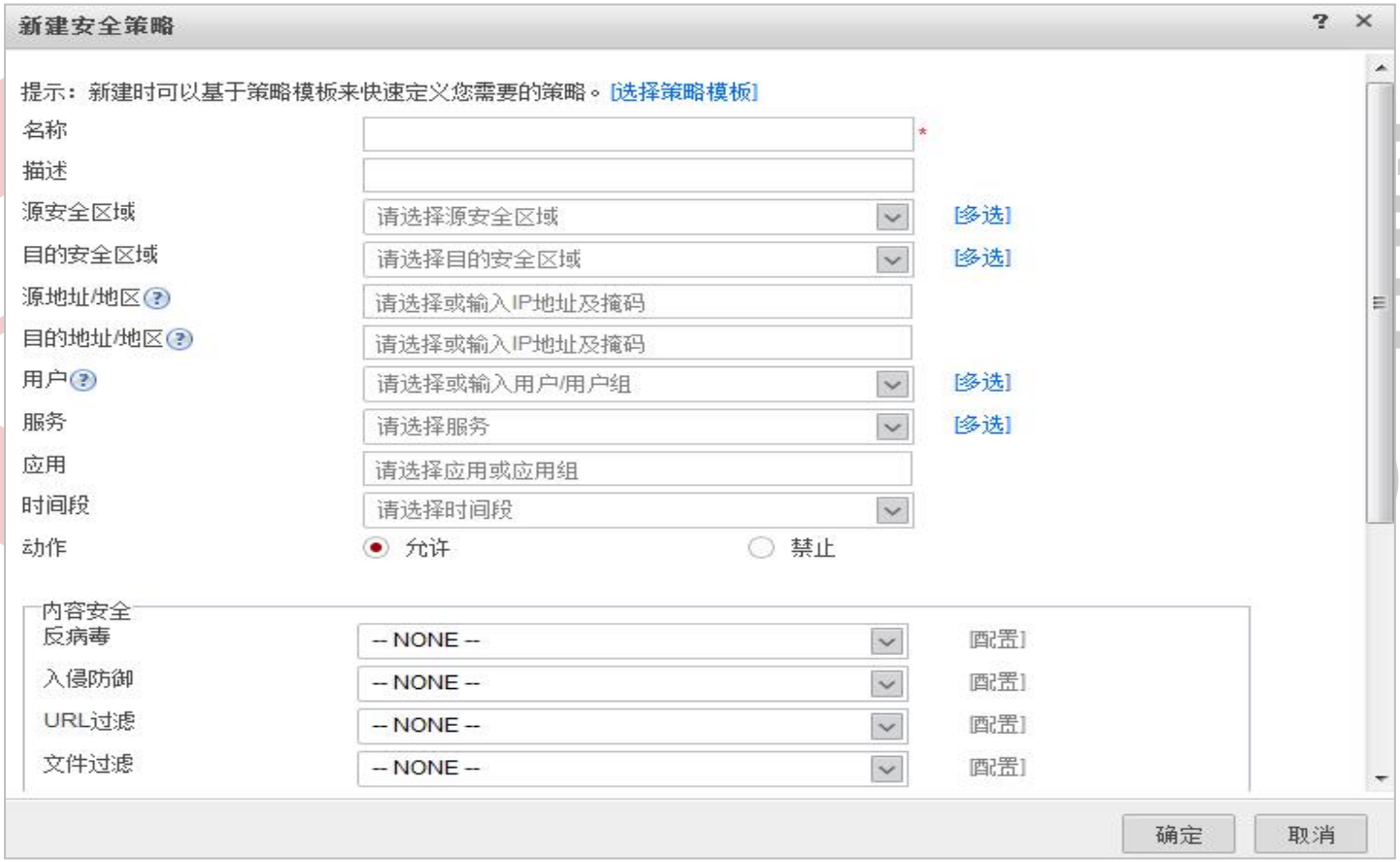
- 应用是指用来执行某一特殊任务或用途的计算机程序。应用组是指多个应用的集合。

配置时间段（WEB）

- 时间段定义了时间范围，定义好的时间段被策略引用后，可以对某一时间段内流经NGFW的流量进行匹配和控制。

配置安全策略（WEB）

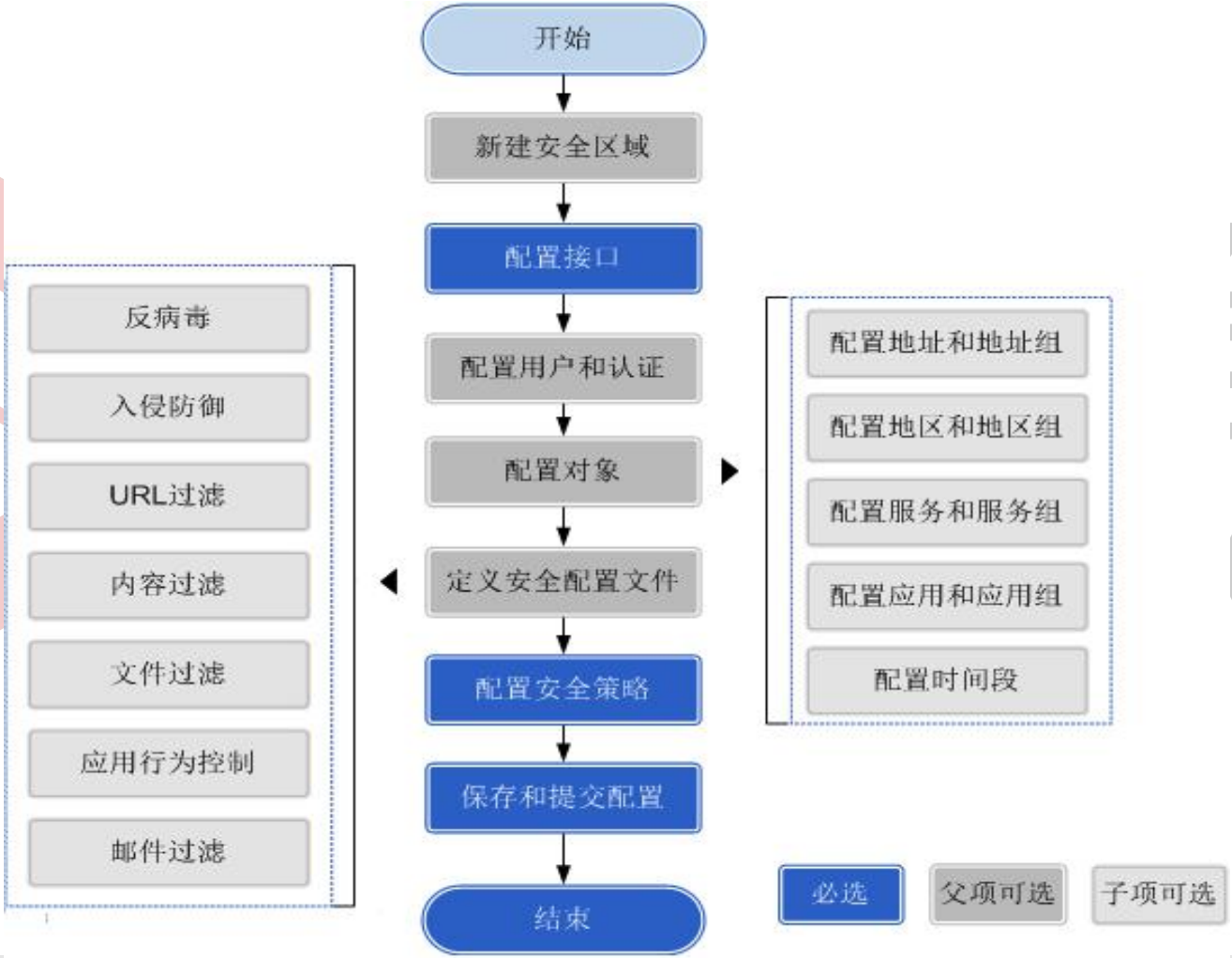
- 在安全策略中可以引用已经创建好的对象。



安全策略配置举例

- 组网需求
  - 在某企业中允许192.168.5.0/24网段的员工访问Internet，但是在此网段中192.168.5.2、192.168.5.3和192.168.5.6的这几台PC对安全性要求较高，不允许上网。

配置安全策略流程



关键配置（命令行）

- 创建拒绝特殊的几个IP地址访问Internet的安全策略规则。

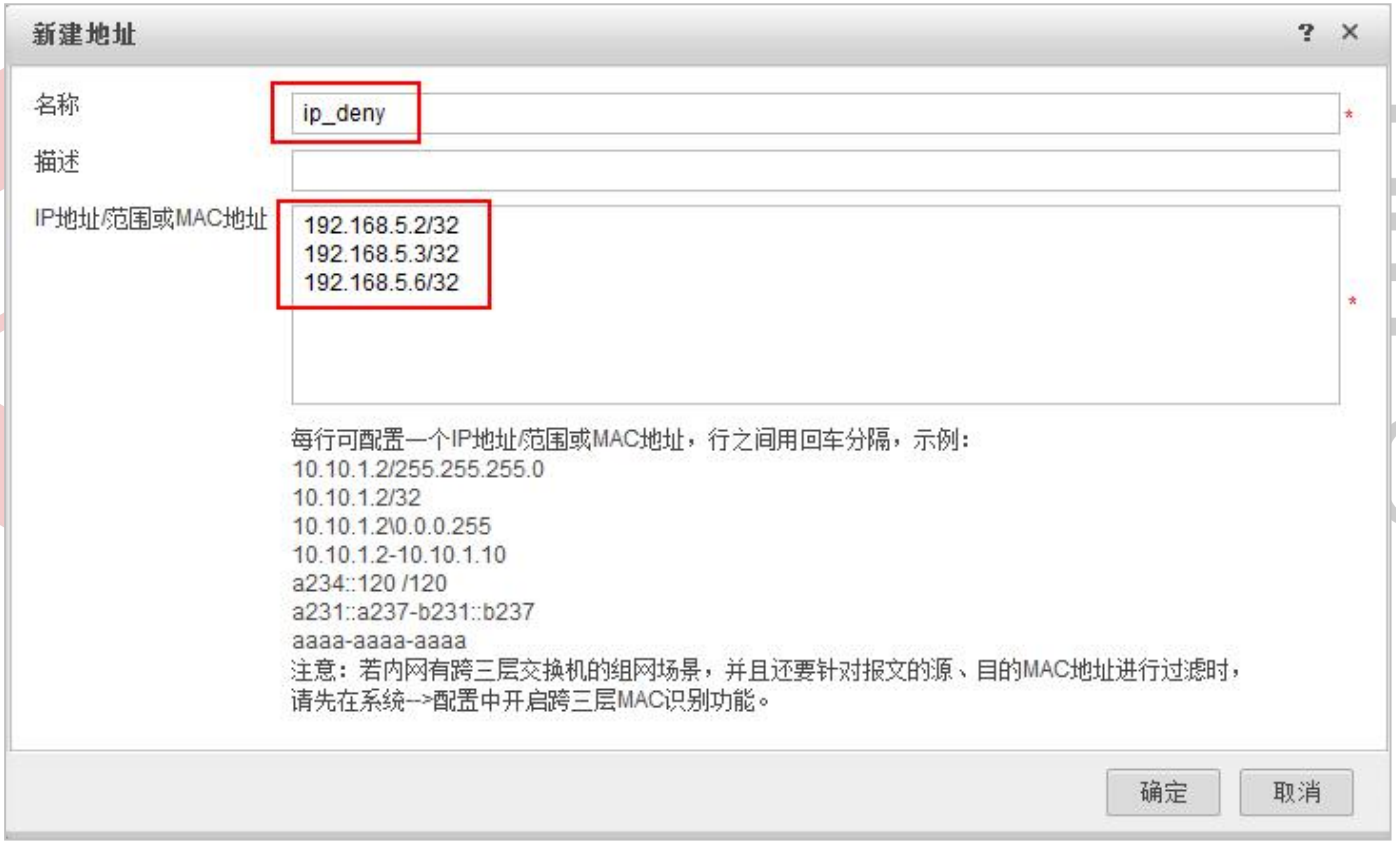
```
[NGFW]security-policy
[NGFW-policy-security]rule name celue
[NGFW-policy-security-rule-celue]source-zone trust
[NGFW-policy-security-rule-celue]destination-zone untrust
[NGFW-policy-security-rule-celue]source-address 192.168.5.2 32
[NGFW-policy-security-rule-celue]source-address 192.168.5.3 32
[NGFW-policy-security-rule-celue]source-address 192.168.5.6 32
[NGFW-policy-security-rule-celue]action deny
```

- 创建允许192.168.5.0/24网段访问Internet的安全策略规则。

```
[NGFW]security-policy
[NGFW-policy-security]rule name celue2
[NGFW-policy-security-rule-celue2]source-zone trust
[NGFW-policy-security-rule-celue2]destination-zone untrust
[NGFW-policy-security-rule-celue2]source-address 192.168.5.0 24
[NGFW-policy-security-rule-celue2]action permit
```

关键配置（WEB）-（1）

- 配置名称为ip_deny的地址组。

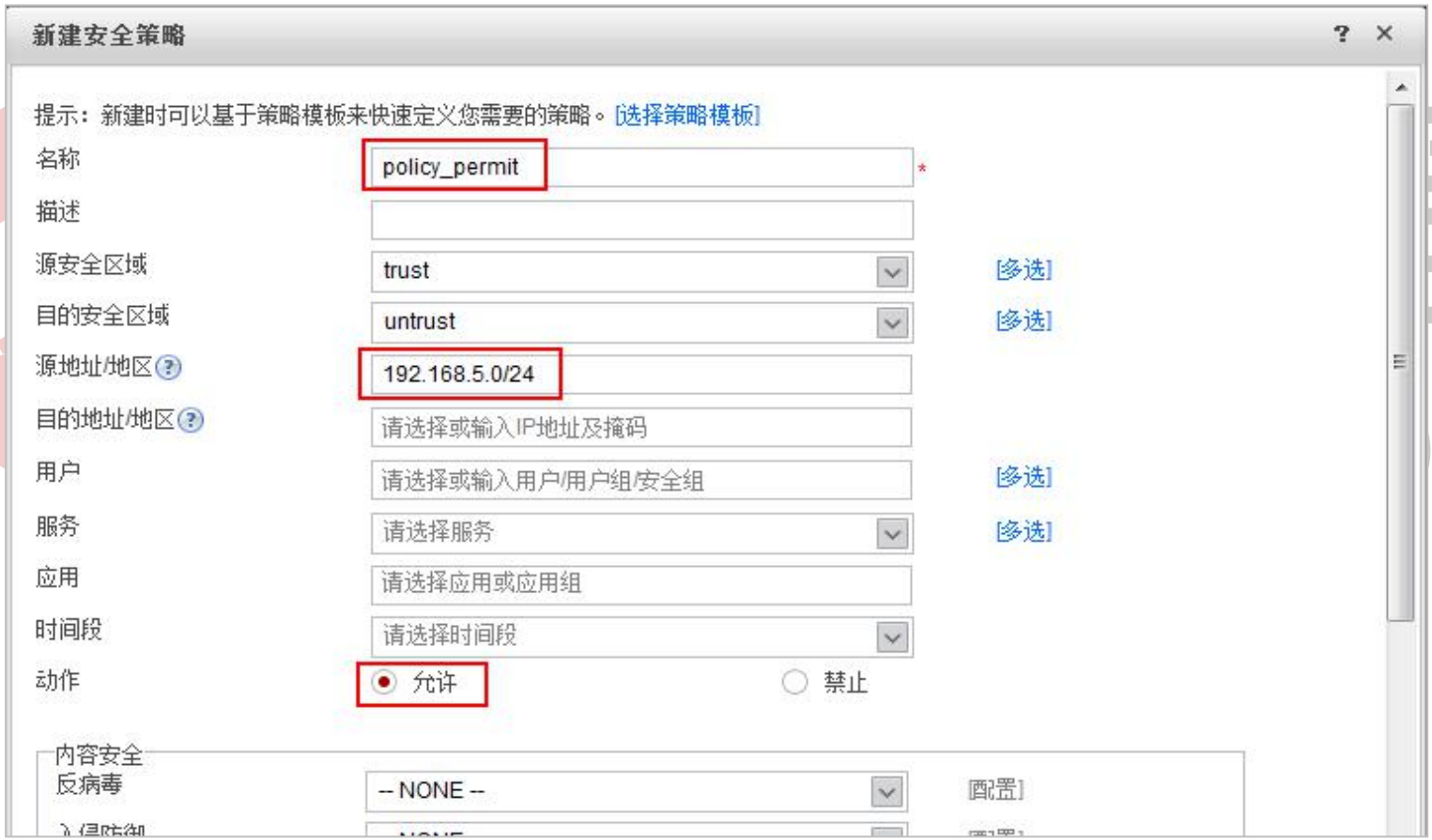


关键配置（WEB）-（2）

- 配置拒绝特殊地址组ip_deny内IP地址访问Internet的安全策略。

关键配置（WEB）-（3）

- 配置允许192.168.5.0/24网段访问Internet的安全策略。



目录

多通道协议技术

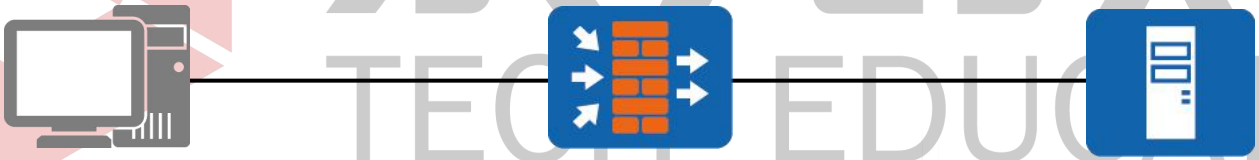
- 单通道协议：通信过程中只需占用一个端口的协议。如：WWW只需占用80端口。
- 多通道协议：通信过程中需占用两个或两个以上端口的协议。如FTP被动模式下需占用21号端口以及一个随机端口。

使用单纯的包过滤方法，如何精确定义（端口级别）多通道协议所使用的端口呢？

遇到使用随机协商端口的协议，单纯的包过滤方法无法进行数据流定义。

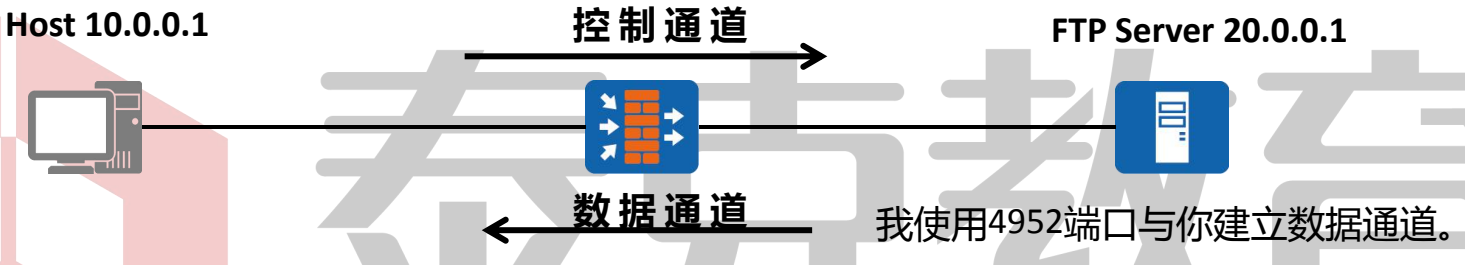
ASPF概述

- ASPF (Application Specific Packet Filter) 是一种高级通信过滤，它检查应用层协议信息并且监控连接的应用层协议状态。对于特定应用协议的所有连接，每一个连接状态信息都将被ASPF维护并用于动态的决定数据包是否被允许通过防火墙或丢弃。



ASPF对多通道协议的支持

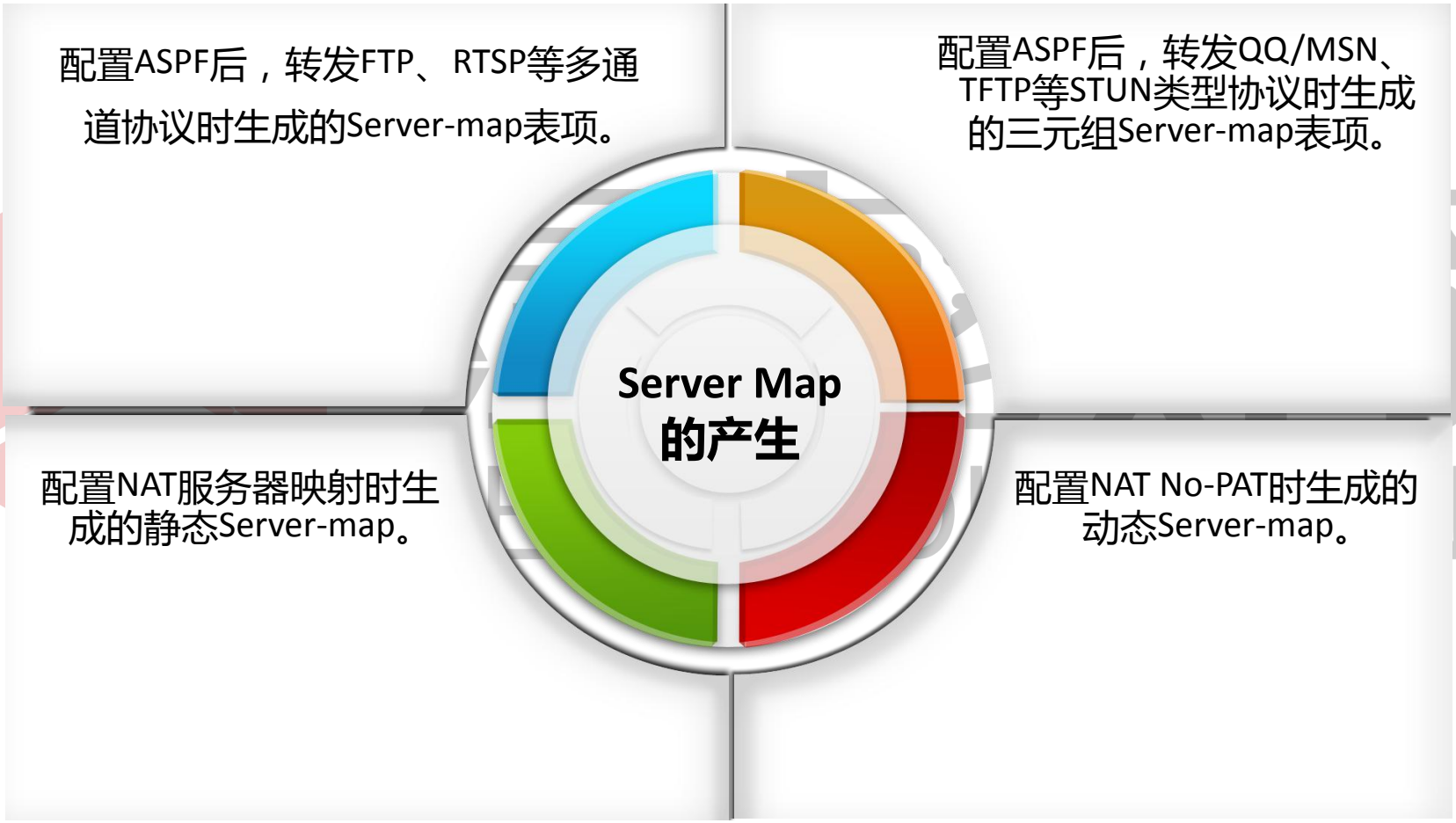
- ASPF（Application Specific Packet Filter）是针对应用层的包过滤。




```
Session表                FTP:10.0.0.1:4927 --> 20.0.0.1:21
                         FTP:10.0.0.1:4926 --> 20.0.0.1:4952
```

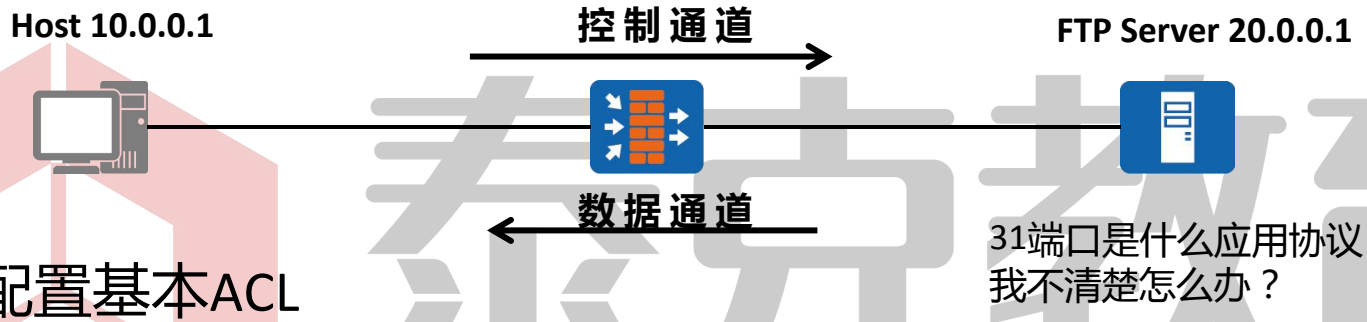
```
ServerMap 表
------------------------------------------------------------
Inside-Address :Port   Global-Address :Port   Pro    AppType   TTL   Left
------------------------------------------------------------
20.0.0.1       :   4952       ---
tcp    FTP    DATA       00:01:00   00:00:47
```

Server Map的产生



端口识别对多通道协议的支持

- 端口识别是把非标准协议端口映射成可识别的应用协议端口。



- 配置基本ACL

```
[NGFW]acl 2000
[NGFW-acl-basic-2000]rule permit source 20.0.0.1 0
```

- 配置端口识别（或端口映射）

```
[NGFW]port-mapping FTP port 31 acl 2000
```

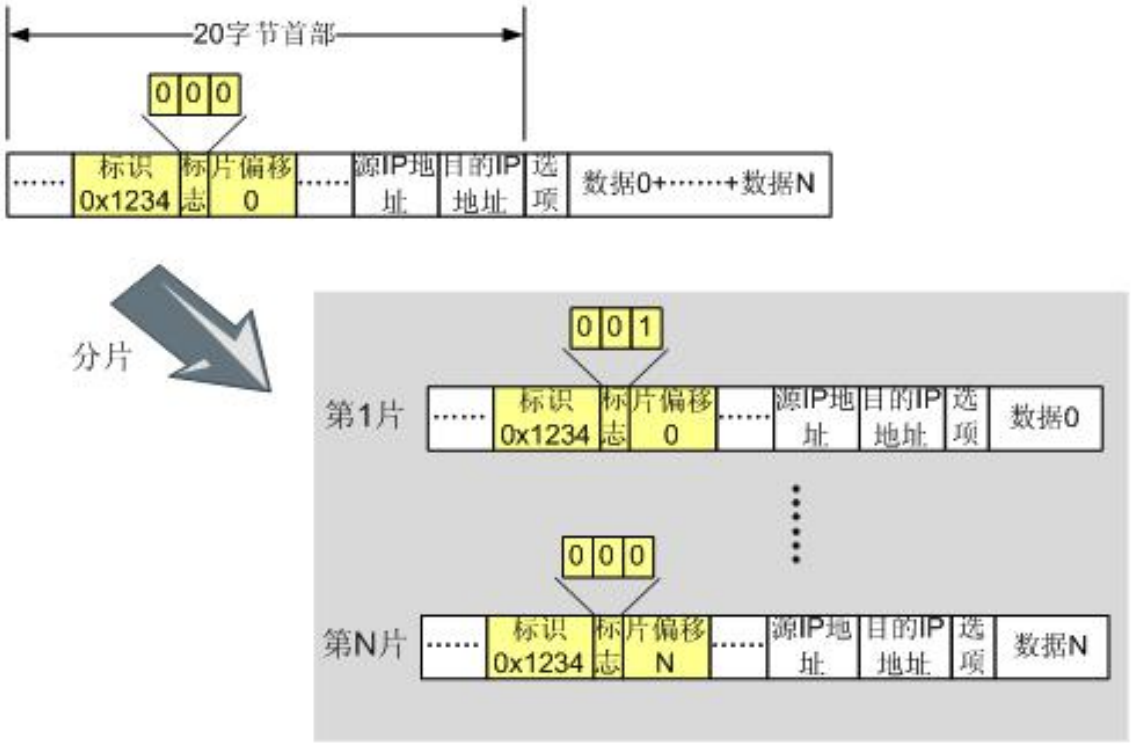
泰克教育

TECH EDUCATION

HUAWEI

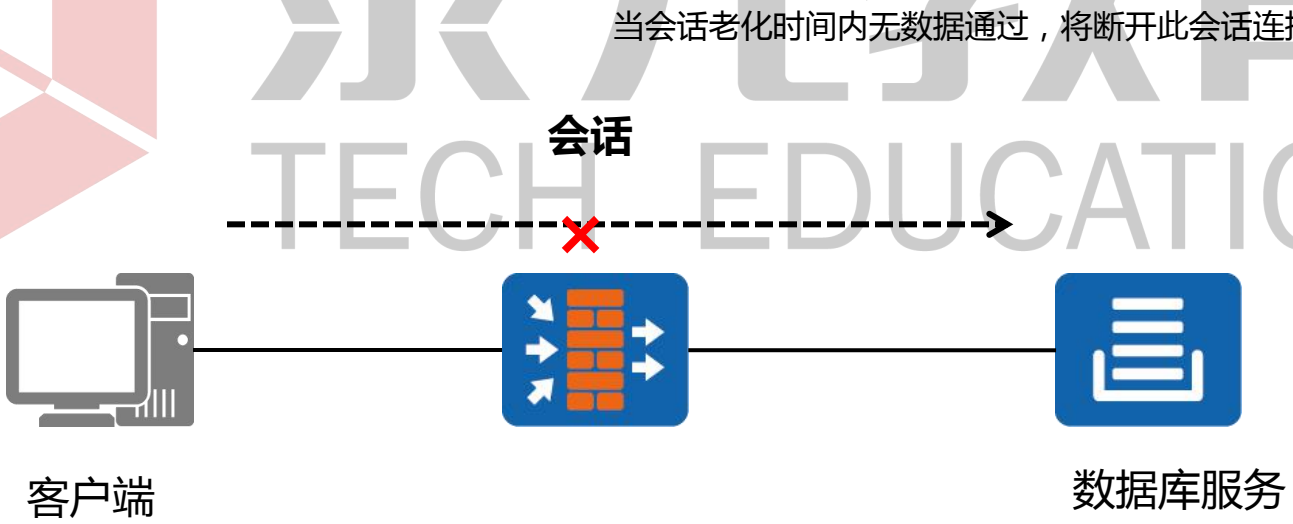
分片缓存

- 分片缓存功能用来缓存先于首片分片报文到达的后续分片报文，避免分片报文被防火墙丢弃。



长连接

- 为什么需要长连接？
  - 防火墙会话表老化机制
  - 会话老化机制给特殊业务带来的问题



思考题

1. 以下哪些情况会下会产生Server Map表？（ ）

   A. 配置NAT No-PAT

   B. 配置NAT服务器映射

   C. 配置ASPF

   D. 配置防火墙的长连接

2. 默认情况下，防火墙有4个安全区域，且不能修改安全级别。（ ）

   A. 正确

   B. 错误

本章总结

- 防火墙包过滤技术原理
- 防火墙转发原理
- 防火墙安全策略应用场景及配置方法

谢谢

www.huawei.com