防火墙安全策略

www.huawei.com

HUAWEI

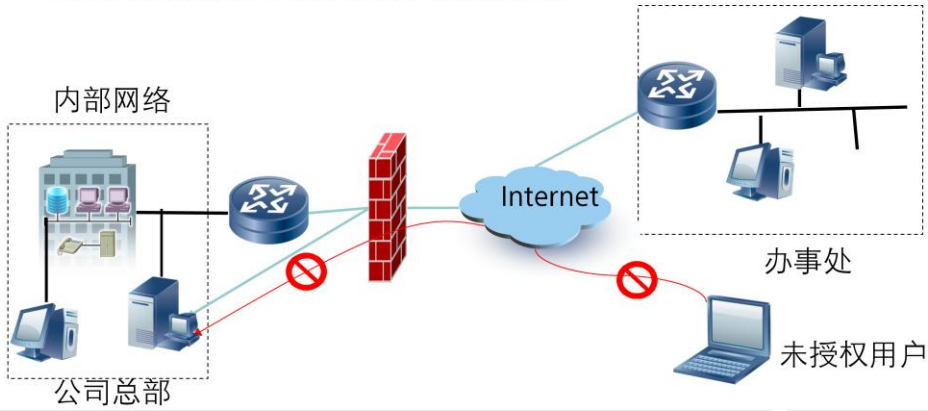
目标

- 学完本课程后，您将能够:
  - 理解防火墙包过滤技术
  - 理解防火墙转发原理
  - 理解防火墙安全策略
  - 掌握防火墙安全策略配置

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。

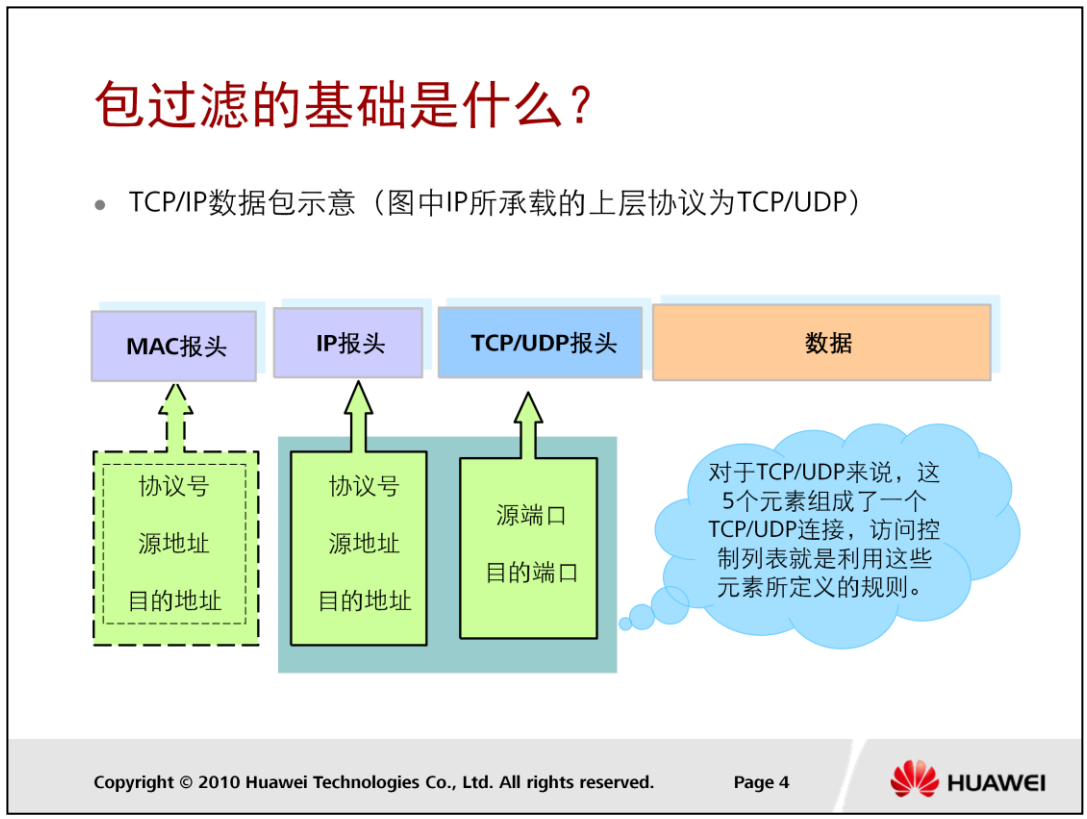


HUAWEI

包过滤作为一种网络安全保护机制，主要用于对网络中各种不同的流量是否转发做一个最基本的控制。

传统的包过滤防火墙对于需要转发的报文，会先获取报文头信息，包括报文的源IP地址、目的IP地址、IP层所承载的上层协议的协议号、源端口号和目的端口号等，然后和预先设定的过滤规则进行匹配，并根据匹配结果对报文采取转发或丢弃处理。

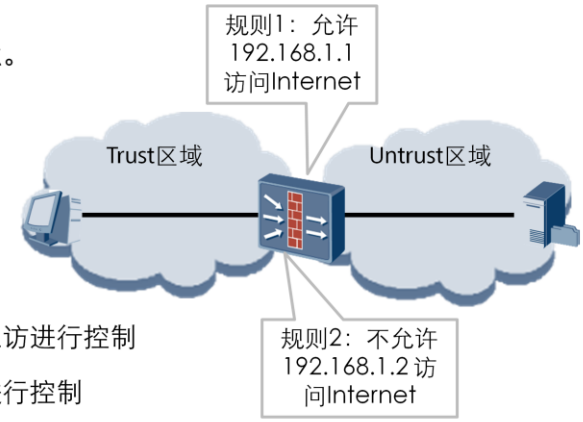
包过滤防火墙的转发机制是逐包匹配包过滤规则并检查，所以转发效率低下。目前防火墙基本使用状态检查机制，将只对一个连接的首包进行包过滤检查，如果这个首包能够通过包过滤规则的检查，并建立会话的话，后续报文将不再继续通过包过滤机制检测，而是直接通过会话表进行转发。



包过滤能够通过报文的源MAC地址、目的MAC地址、源IP地址、目的IP地址、源端口号、目的端口号、上层协议等信息组合定义网络中的数据流，其中源IP地址、目的IP地址、源端口号、目的端口号、上层协议就是在状态检测防火墙中经常所提到的五无组，也是组成TCP/UDP连接非常重要的五个元素。

防火墙安全策略

- 定义
  - 安全策略是按一定规则检查数据流是否可以通过防火墙的基本安全控制机制。
  - 规则的本质是包过滤。

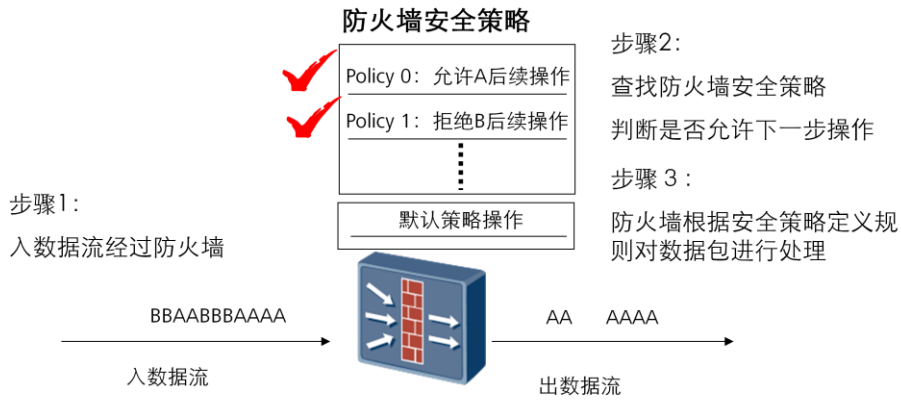


- 主要应用
  - 对跨防火墙的网络互访进行控制
  - 对设备本身的访问进行控制

防火墙的基本作用是保护特定网络免受“不信任”的网络的攻击，但是同时还必须允许两个网络之间可以进行合法的通信。安全策略的作用就是对通过防火墙的数据流进行检验，符合安全策略的合法数据流才能通过防火墙。

通过防火墙安全策略可以控制内网访问外网的权限、控制内网不同安全级别的子网间的访问权限等。同时也能够对设备本身的访问进行控制，例如限制哪些IP地址可以通过Telnet和Web等方式登录设备，控制网管服务器、NTP服务器等与设备的互访等。

防火墙安全策略的原理



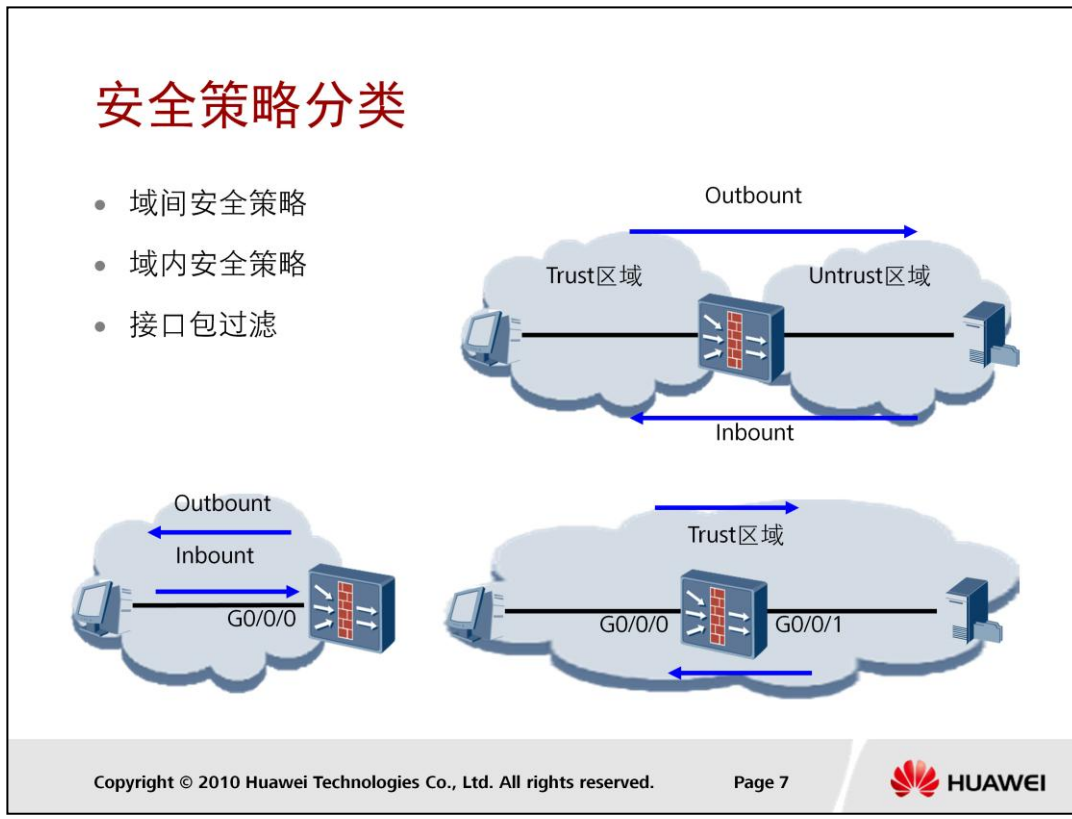
- 防火墙安全策略作用：

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。

防火墙安全策略定义数据流在防火墙上的处理规则，防火墙根据规则对数据流进行处理。因此，防火墙安全策略的核心作用是：根据定义的规则对经过防火墙的流量进行筛选，由关键字确定筛选出的流量如何进行下一步操作。

在防火墙应用中，防火墙安全策略是对经过防火墙的数据流进行网络安全访问的基本手段，决定了后续的应用数据流是否被处理。安全策略根据通过报文的源地址、目的地址、端口号、上层协议等信息组合定义网络中的数据流。

思考：五元组在安全策略中是如何进行匹配的?

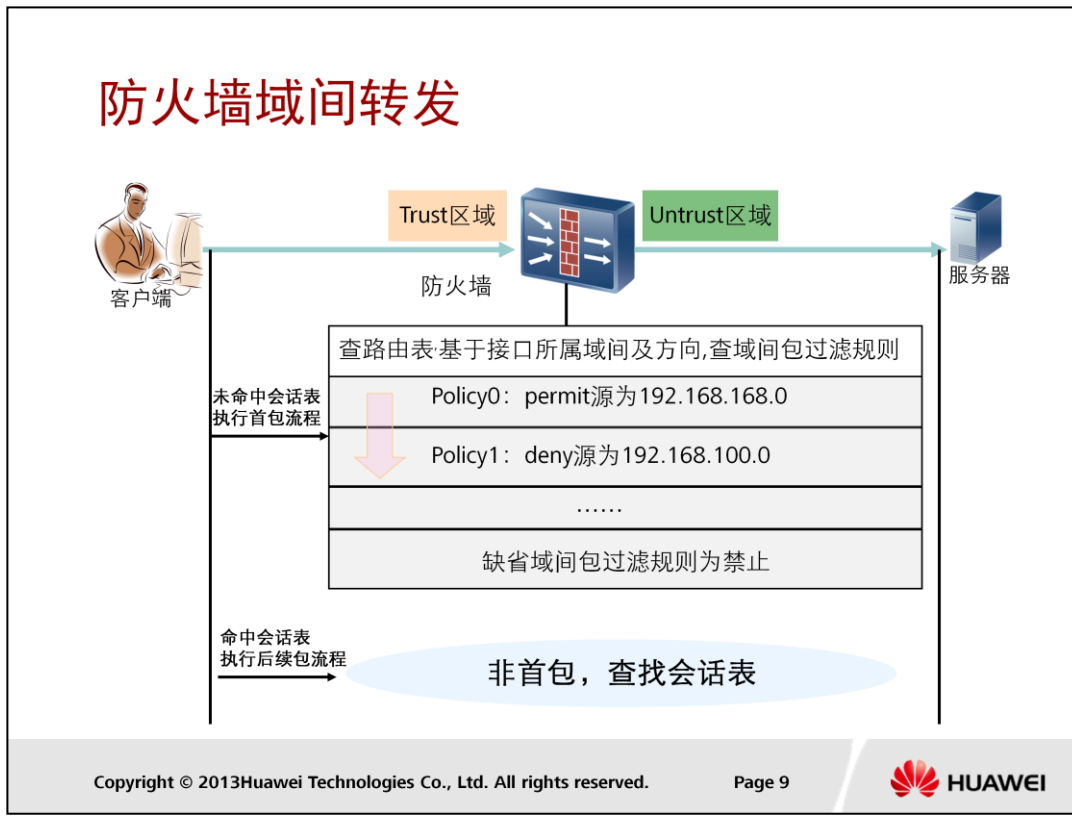


域间安全策略用于控制域间流量的转发（此时称为转发策略），适用于接口加入不同安全区域的场景。域间安全策略按IP地址、时间段和服务（端口或协议类型）、用户等多种方式匹配流量，并对符合条件的流量进行包过滤控制（permit/deny）或高级的UTM应用层检测。域间安全策略也用于控制外界与设备本身的互访（此时称为本地策略），按IP地址、时间段和服务（端口或协议类型）等多种方式匹配流量，并对符合条件的流量进行包过滤控制（permit/deny），允许或拒绝与设备本身的互访。

缺省情况下域内数据流动不受限制，如果需要进行安全检查可以应用域内安全策略。与域间安全策略一样可以按IP地址、时间段和服务（端口或协议类型）、用户等多种方式匹配流量，然后对流量进行安全检查。例如：市场部和财务部都属于内网所在的安全区域Trust，可以正常互访。但是财务部是企业重要数据所在的部门，需要防止内部员工对服务器、PC等的恶意攻击。所以在域内应用安全策略进行IPS检测，阻断恶意员工的非法访问。

当接口未加入安全区域的情况下，通过接口包过滤控制接口接收和发送的IP报文，可以按IP地址、时间段和服务（端口或协议类型）等多种方式匹配流量并执行相应动作（permit/deny）。基于MAC地址的包过滤用来控制接口可以接收哪些以太网帧，可以按MAC地址、帧的协议类型和帧的优先级匹配流量并执行相应动作（permit/deny）。硬件包过滤是在特定的二层硬件接口卡上实现的，用来控制接口卡上的接口可以接收哪些流量。硬件包过滤直接通过硬件实现，所以过滤速度更快。

目录

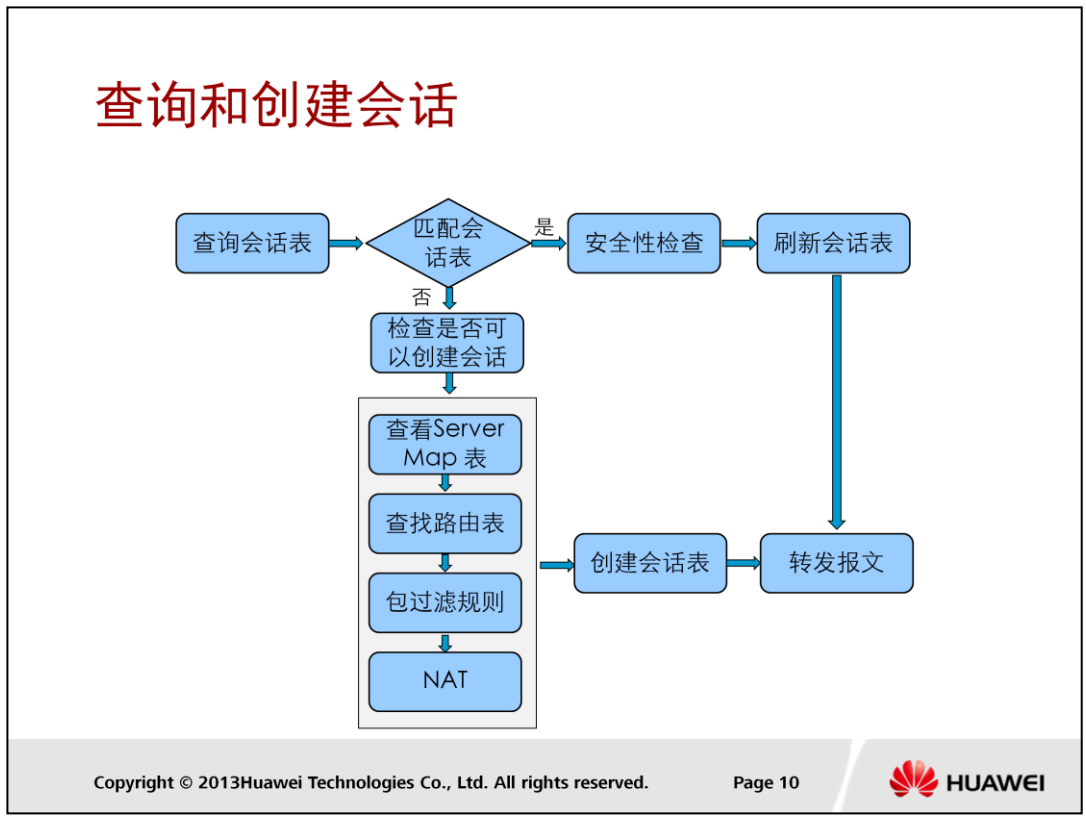


早期包过滤防火墙采取的是“逐包检测”机制，即对设备收到的所有报文都根据包过滤规则每次都进行检查以决定是否对该报文放行。这种机制严重影响了设备转发效率，使包过滤防火墙成为网络中的转发瓶颈。

于是越来越多的防火墙产品采用了“状态检测”机制来进行包过滤。“状态检测”机制以流量为单位来对报文进行检测和转发，即对一条流量的第一个报文进行包过滤规则检查，并将判断结果作为该条流量的“状态”记录下来。对于该流量的后续报文都直接根据这个“状态”来判断是转发还是丢弃，而不会再次检查报文的数据内容。这个“状态”就是我们平常所述的会话表项。这种机制迅速提升了防火墙产品的检测速率和转发效率，已经成为目前主流的包过滤机制。

在防火墙一般是检查IP报文中的五个元素，又称为“五元组”，即源IP地址和目的IP地址，源端口号和目的端口号，协议类型。通过判断IP数据报文报文的五元组，就可以判断一条数据流相同的IP数据报文。

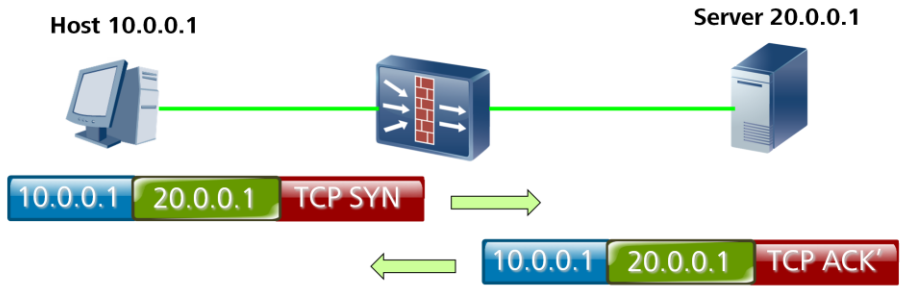
其中TCP协议的数据报文，一般情况下在三次握手阶段除了基于五元组外，还会计算及检查其它字段。三次握手建立成功后，就通过会话表中的五元组对设备收到后续报文进行匹配检测，以确定是否允许此报文通过。



可以看出，对于已经存在会话表的报文的检测过程比没有会话表的报文要短很多。而通常情况下，通过对一条连接的首包进行检测并建立会话后，该条连接的绝大部分报文都不再需要重新检测。这就是状态检测防火墙的“状态检测机制”相对于包过滤防火墙的“逐包检测机制”的改进之处。这种改进使状态检测防火墙在检测和转发效率上有迅速提升。

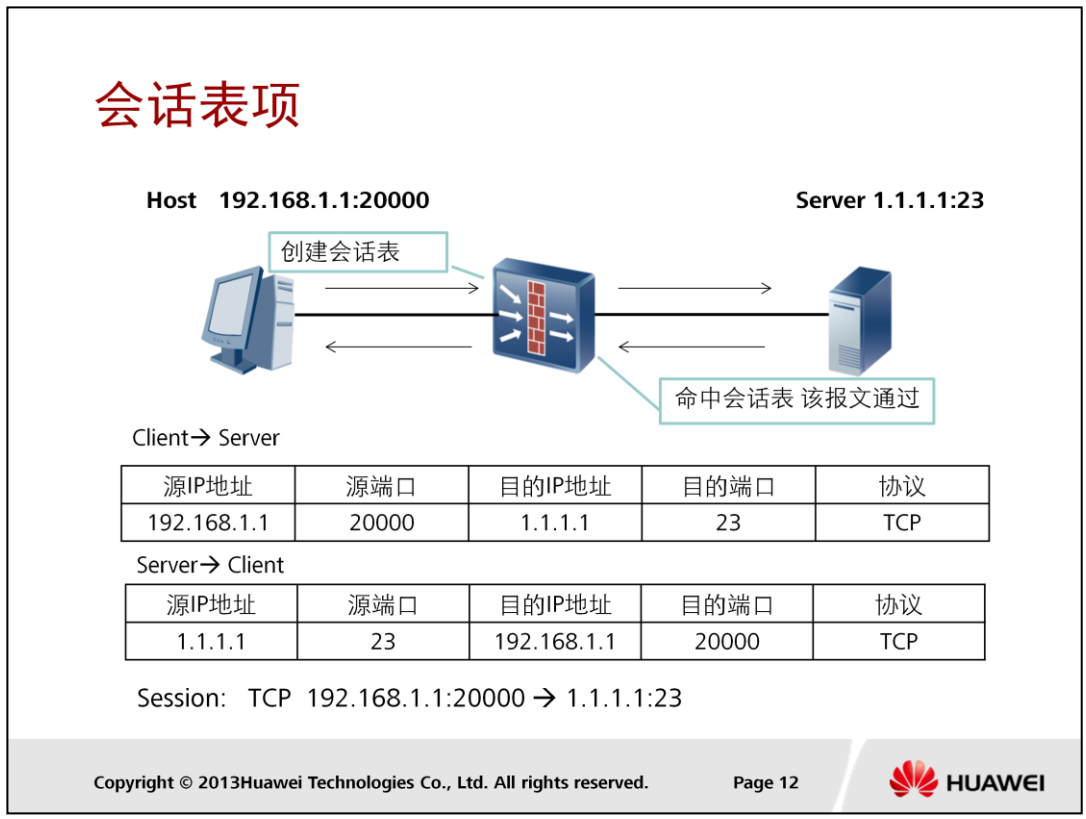
状态检测机制

- 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。



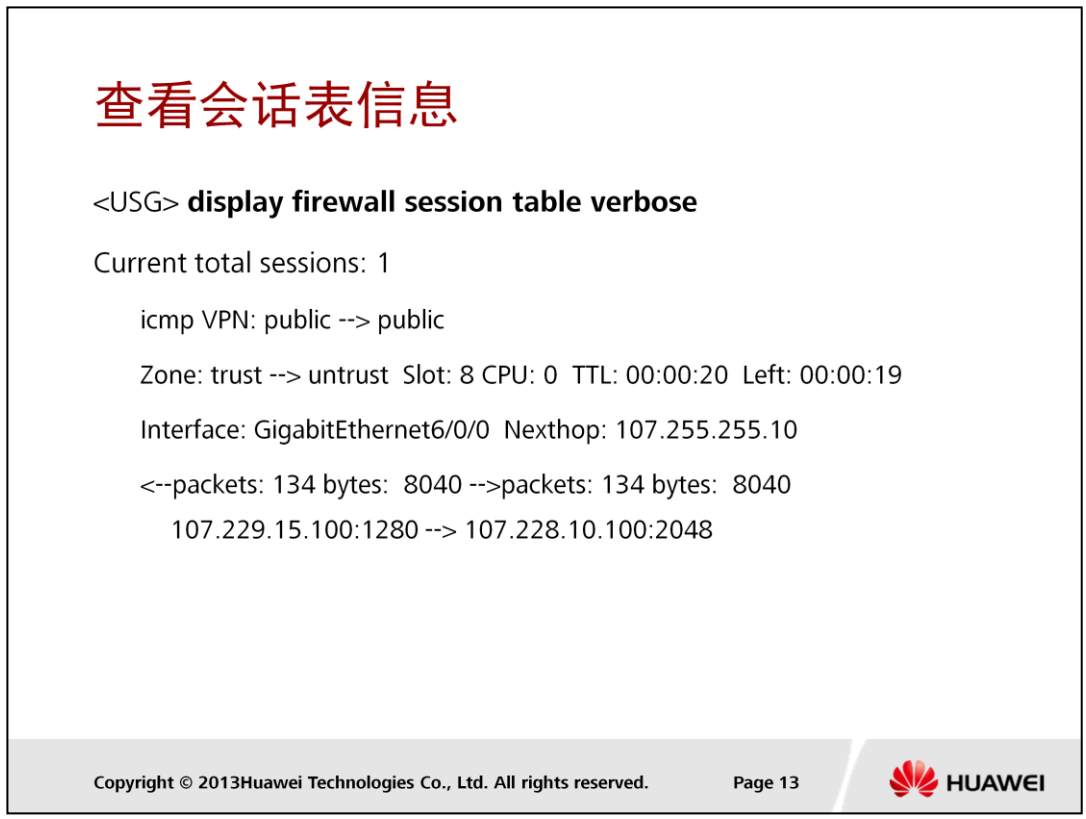
HUAWEI

- 对于TCP报文
  - 开启状态检测机制时，首包（SYN报文）建立会话表项。对除SYN报文外的其他报文，如果没有对应会话表项（设备没有收到SYN报文或者会话表项已老化），则予以丢弃，也不会建立会话表项。
  - 关闭状态检测机制时，任何格式的报文在没有对应会话表项的情况下，只要通过各项安全机制的检查，都可以为其建立会话表项。
- 对于UDP报文
  - UDP是基于无连接的通信，任何UDP格式的报文在没有对应会话表项的情况下，只要通过各项安全机制的检查，都可以为其建立会话表项。
- 对于ICMP报文
  - 开启状态检测机制时，没有对应会话的ICMP应答报文将被丢弃。
  - 关闭状态检测机制时，没有对应会话的应答报文以首包形式处理



会话是状态检测防火墙的基础，每一个通过防火墙的数据流都会在防火墙上建立一个会话表项，以五元组（源目的IP地址、源目的端口、协议号）为Key值，通过建立动态的会话表提供域间转发数据流更高的安全性。

- 会话表包括五个元素：
  - 源IP地址
  - 源端口
  - 目的IP地址
  - 目的端口
  - 协议号



display firewall session table [verbose]

用来显示系统当前的会话表项信息，verbose参数来控制是否显示详细的信息。

- icmp 表示会话表的应用类型为ICMP协议。
- trust --> untrust 表示从Trust区域到Untrust区域方向的流量建立的会话。
- Interface 表示流量的出接口。
- Nexthop 表示流量的下一跳地址。
- <--packets 表示反向报文命中的会话数，即从Untrust到Trust方向的报文数。

说明： 在NAT或VPN应用中，反向会话的报文统计数通常会有延时。

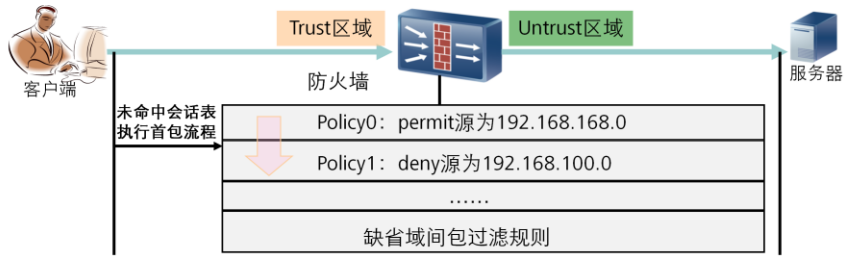
- -->packets 表示正向报文命中的会话数，即从Trust到Untrust方向的报文数。
- 107.229.15.100:1280 表示源IP地址和源端口
- 107.228.10.100:2048 表示目的IP地址和目的端口

<USG> reset firewall session table

- 清除系统当前会话表项。
- Reset Session表项操作得谨慎，因为会导致在运行业务中断。

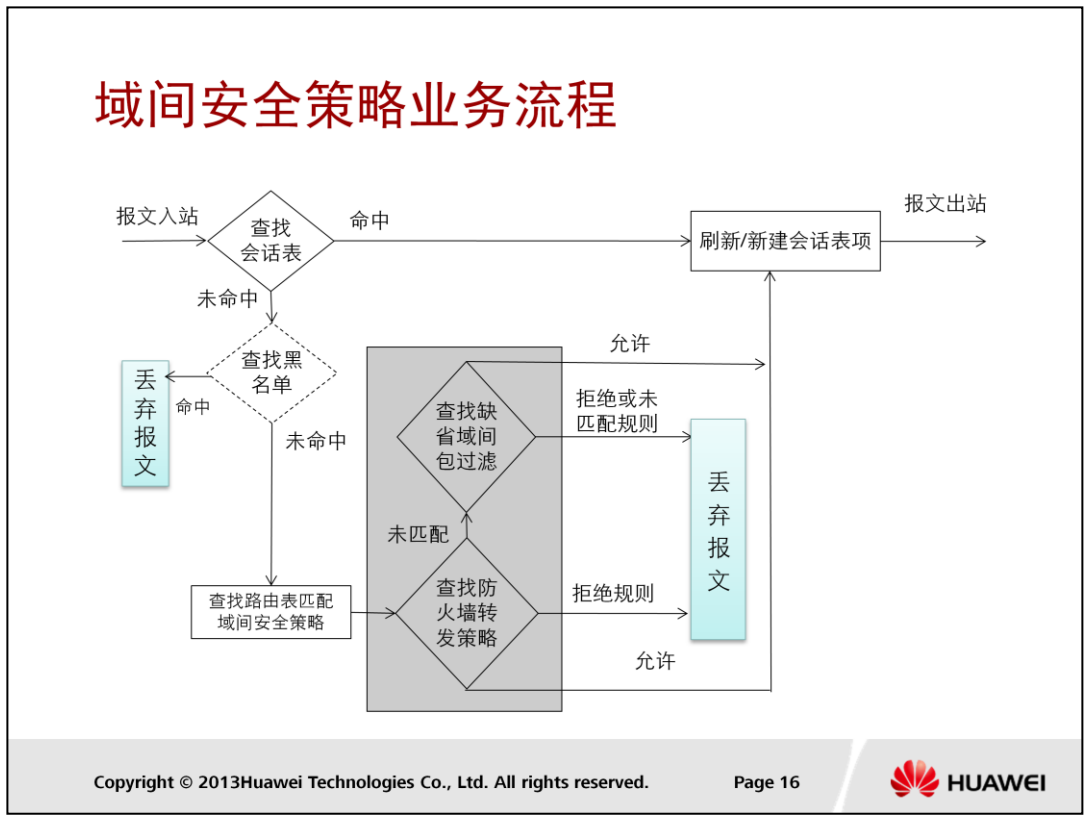
目录

域间安全策略的匹配原则



- 域间安全策略的分类
  - 域间缺省包过滤
  - 转发策略
  - 本地策略

- 域间缺省包过滤
  - 当数据流无法匹配域间安全策略时，会按照域间缺省包过滤规则来转发或丢弃该数据流的报文。
- 转发策略
  - 转发策略是指控制哪些流量可以经过设备转发的域间安全策略，对域间（除Local域外）转发流量进行安全检查，例如控制哪些Trust域的内网用户可以访问Untrust域的Internet。
- 本地策略
  - 本地策略是指与Local安全区域有关的域间安全策略，用于控制外界与设备本身的互访。



报文入站后，将首先匹配会话表，如果命中会话表，将进入后续包处理流程，刷新会话表时间，并直接根据会话表中的出接口，转发数据。

报文入站后，将首先匹配会话表，如果没有命中会话表，将进入首包包处理流程。依次进行黑名单检查，查找路由表，匹配域间安全策略，新建会话表，转发数据。

黑名单的实现原理就是：设备上建立一个黑名单表。对于接收到的报文的源IP地址存在于黑名单中，就将该报文予以丢弃。

黑名单分类：

- 静态黑名单

管理员可以通过命令行或Web方式手工逐个将IP地址添加到黑名单中。

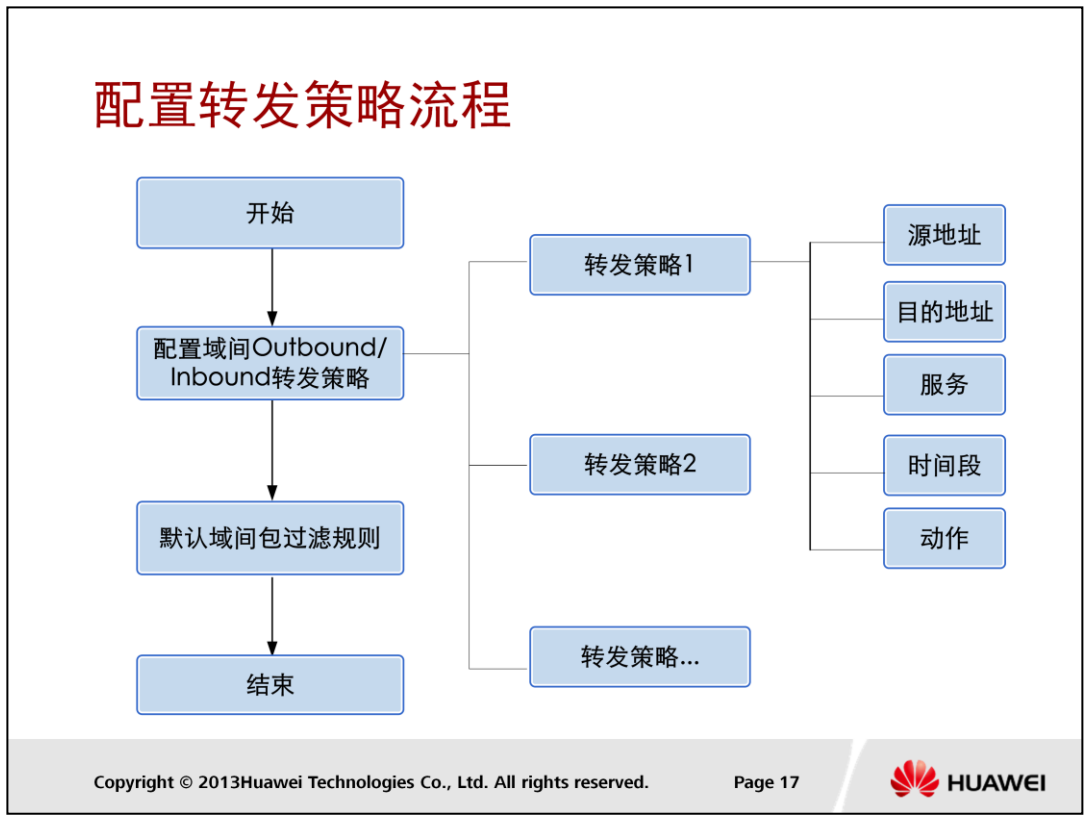
- 动态黑名单

转发策略和缺省域间包过滤优先级

转发策略优先于缺省域间包过滤匹配。设备将首先查找域间的转发策略，如果没有找到匹配项将匹配缺省包过滤进行处理。

- 刷新会话表

刷新会话表主要是刷新会话表老化时间，老化时间决定会话在没有相应的报文匹配的情况下，何时被系统删除。



- 转发策略的配置流程如图所示。
- 有两种思路来配置转发策略，根据需要选择。
  - 思路1：对安全性要求不高，开放缺省转发策略，然后只把个别需要拒绝的流量拒绝掉，出于安全性考虑不建议这种方式。
  - 思路2：关闭缺省转发策略，然后根据需要配置严格的转发策略。

举例：

policy interzone trust untrust outbound

policy 0

action permit

policy source 192.168.168.0 0.255.0.255

policy service service-set http

同一个域间包过滤策略视图下可以为不同的流量创建不同的策略。缺省情况下，越先配置的策略，优先级越高，越先匹配报文。一旦匹配到一条Policy，就直接按照该Policy的定义处理报文，不再继续往下匹配。各个**policy**之间的优先级关系可以通过命令进行调整。

在包过滤策略视图下执行**policy** *policy-id* { **enable** | **disable** }，启用或者禁用一条自定义策略。

- source-wildcard点分十进制格式的通配符。
    - 例如：192.168.1.0 0.0.0.255，这里的0.0.0.255就是通配符。并且通配符的二进制形式支持1不连续，例如：0.255.0.255。 通配符转换为二进制后，为“0”的位是匹配值（源IP）中需要匹配的位，为“1”的位表示不需要关注。0.0.0.255的二进制形式是00000000 00000000 00000000 11111111，所以源IP地址是192.168.1.*的报文均能匹配到。
- 0通配符，表示主机。
- mask
    - mask-address 指定掩码。 点分十进制格式，形如255.255.255.0表示掩码长度为24。
    - mask mask-len 指定掩码长度。 整数形式，取值范围是1～32。
- address-set 指定地址集作为源IP地址。 可以指定1～256个地址集。
    - address-set-name 地址集名称。 字符串形式，不支持空格，支持除“-”、“?”和“,”以外的任意字符，长度范围是1～31个字符，不能以数字开头。
- range 指定源IP地址范围。 -
    - begin-address 起始IP地址。 点分十进制格式。
    - end-address 结束IP地址。 点分十进制格式。
- any 指定策略的源IP地址为任意IP地址。 -

如何使用反掩码

- 反掩码和子网掩码格式相似，但取值含义不同
  - 0表示对应的IP地址位需要比较
  - 1表示对应的IP地址位忽略比较

怎样利用 IP 地址 和
反掩码wildcard-mask 来表示
一个网段?

- 反掩码和IP地址结合使用，可以描述一个地址范围

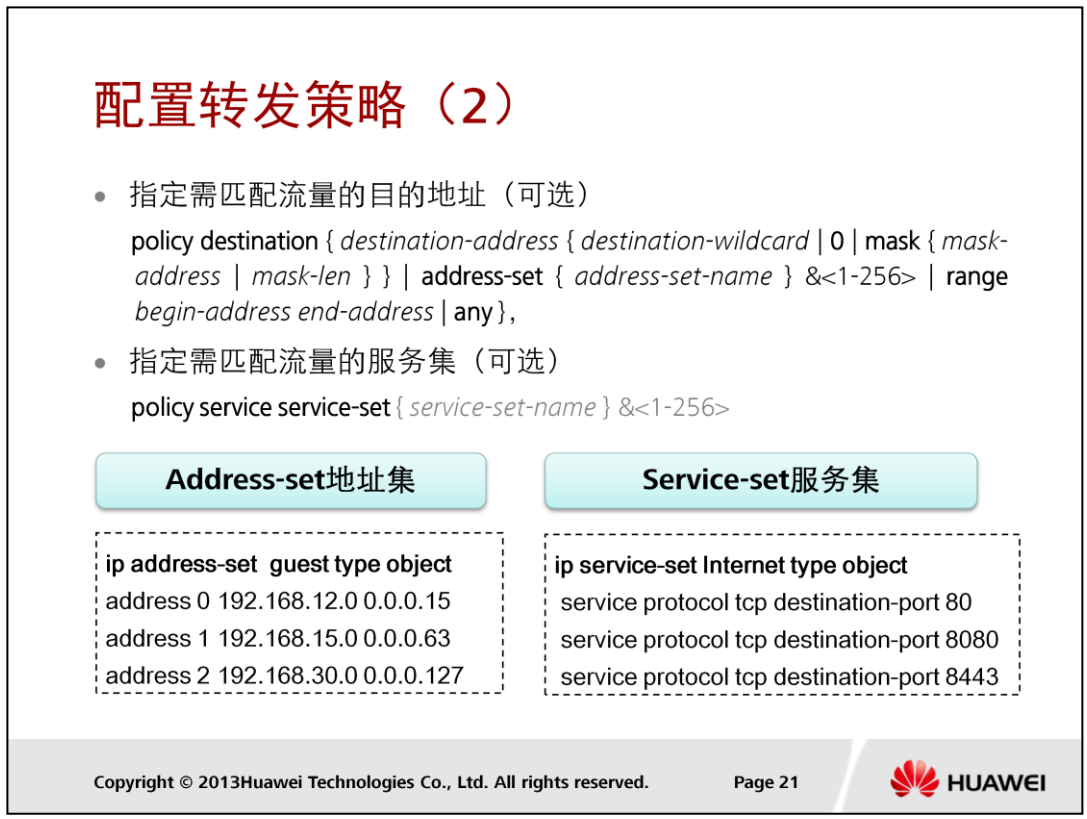
0	0	0	255	只比较前24位
0	0	3	255	只比较前22位
0	255	255	255	只比较前8位

HUAWEI

举例：

192.168.10.0 0.0.0.255表示一个网段

192.168.10.1 0表示一个IP



为简化配置和维护，防火墙支持引用地址集和服务集。除了提升配置和维护效率外，还使规则项更具可读性。

通过源/目的IP地址对流量进行控制时，可以将连续或不连续的地址加入地址集，然后在策略或规则中引用。

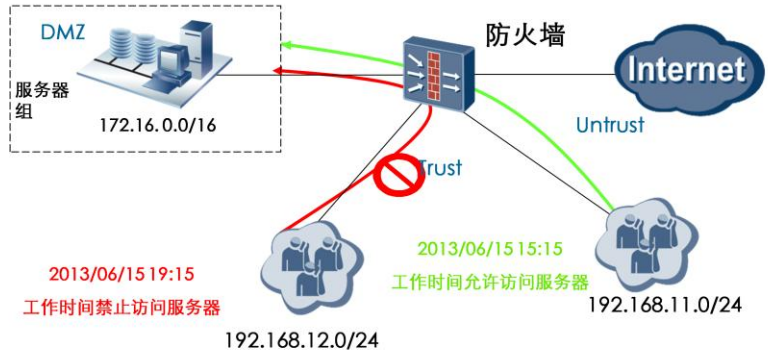
通过流量的服务类型（端口或协议类型）对流量进行控制时，可以使用预定义的知名服务集，也可以根据端口等信息创建自定义服务集，然后在策略或规则中引用。预定义服务集是系统缺省已经存在可以直接选择的服务类型。预定义服务通常都是知名协议，例如HTTP、FTP、Telnet等。自定义服务集是管理员通过指定端口号等信息来自行定义一些协议类型，也可以是各类服务集的组合。

地址集和服务集支持2种type，即object和group。type为group时，可以添加地址集或服务集作为成员。

配置转发策略（3）

- 配置策略生效的时间段（可选）

  policy time-range *time-name*



- 配置对匹配流量的包过滤动作

  action { permit | deny }

如果需要对某一时间内发生的流量进行匹配和控制，可以通过使用基于时间段的访问控制列表。

在网络应用中，比较常见的应用是按照时间段开放某些网络应用，例如：上班时间不开放服务器某些端口，上班时间局域网的某些用户不能访问Internet等。这种特殊的应用前面所介绍的各种访问控制列表类型都无法满足要求，基于时间段访问控制列表可以精确的限定某个访问控制列表的生效时间，解决了访问控制列表在时间上一刀切的问题。

在定义时间段访问控制列表前，首先要在防火墙上定义一个时间段。

时间段配置

- **创建时间段**

  time-range *time-name* { *start-time* **to** *end-time days* | **from** *time1 date1* [**to** *time2 date2*] }

操作符及语法	意义
HH:MM	From 某时间 To某时间
YYYY/MM/DD	From 某日期 To某日期
Mon/Tue/Wed/Thu/Fri/Sat/Sun	星期一/二/三/四/五/六/日
daily	一星期中的每天
off-day	休息日（星期六/日）
Working-day	工作日（星期一 至 星期五）

Time-range时间范围操作符，支持2种表现方式。一种是绝对时间段，即起止日期的时间段，另一种是周期时间段，即星期方式的时间段。

配置举例：

time-range work-policy1 08:00 to 18:00 working-day

time-range work-policy2 from 08:00 2013/01/01 to 18:00 2013/12/31

policy interzone trust untrust outbound

policy 1

Policy source 192.168.11.0 0.0.0.255

policy time-range work-policy1

policy 2

Policy source 192.168.12.0 0.0.0.255

policy time-range work-policy2

举例：

policy interzone trust local inbound

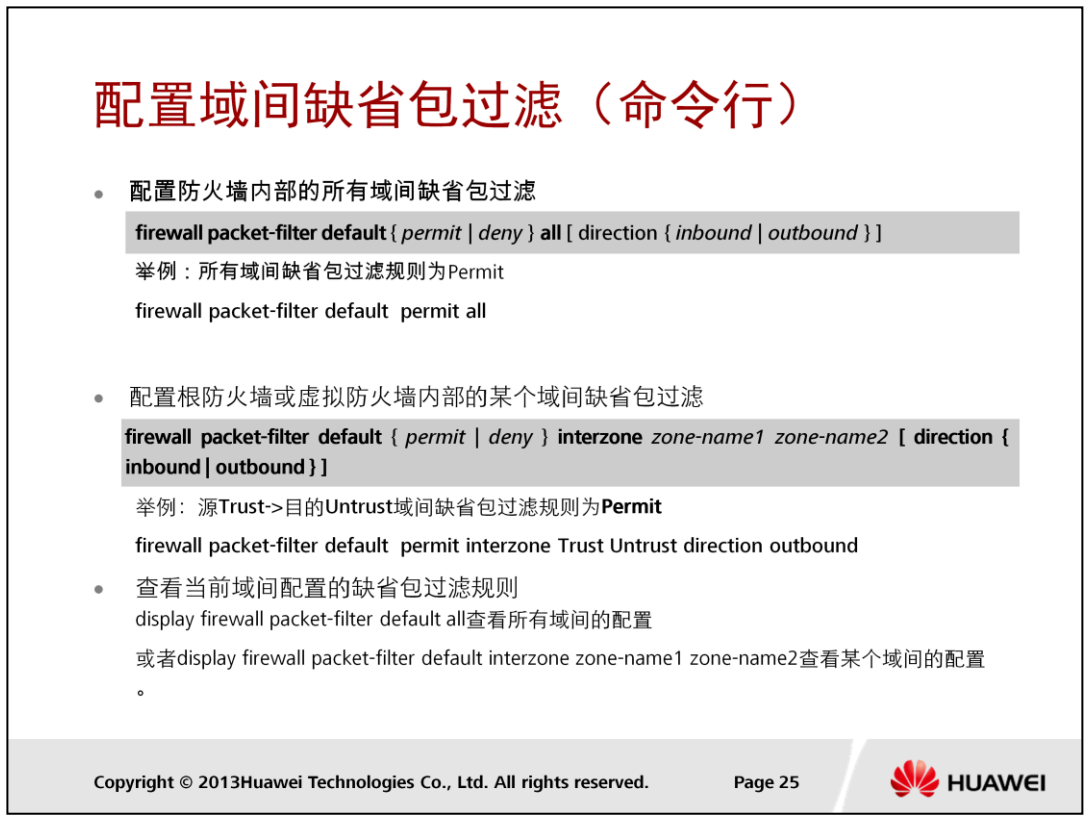
policy 0

action permit

policy source 10.1.1.1 0

policy service service-set telnet

在域间安全策略视图下执行policy policy-id { enable | disable }，启用或者禁用一条策略。



USG2200/5100/5500缺省出厂配置:

- 允许通过:
  - Local域到其他任意安全区域Outbound方向的报文
  - Trust域到Local域的Outbound和Inbound报文；
- 禁止通过：
  - 其他安全区域间的所有方向都禁止报文通过。

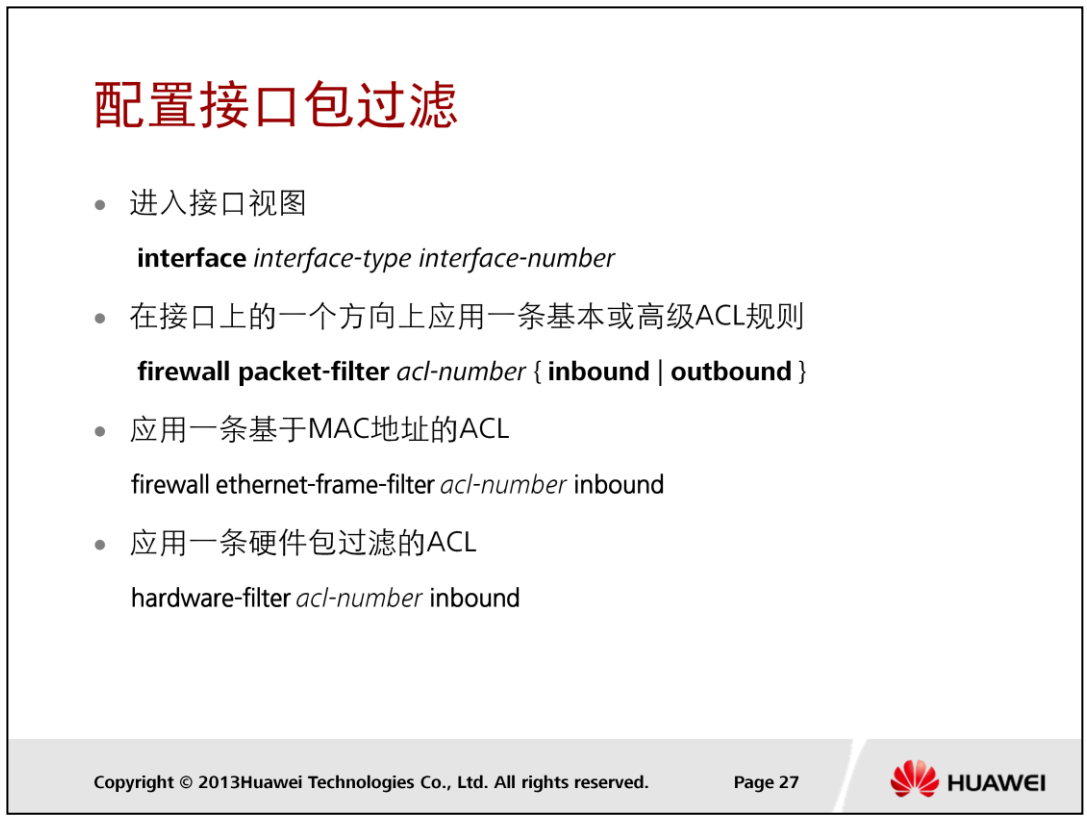
USG2200/USG5100 BSR/HSR缺省出厂配置：

- 允许通过:
  - 所有安全区域间的所有方向的报文

举例：

```
policy zone trust
policy 0
action deny
policy service service-set ftp
policy source 1.1.1.1 0
policy destination 10.1.1.1 0
```

在域内安全策略视图下执行policy policy-id { enable | disable }，启用或者禁用一条策略。



ACL(Access Control List),访问控制列表是一系列有顺序的规则组的集合，这些规则根据数据包的源地址、目的地址、端口号等来描述。ACL通过规则对数据包进行分类，这些规则应用到路由设备上，路由设备根据这些规则判断哪些数据包可以接收，哪些数据包需要拒绝。

- ACL定义的数据流有很大区别：
  - 基本ACL2000～2999仅使用源地址信息进行流量匹配。
  - 高级ACL3000～3999可以使用数据包的源地址、目的地址、IP承载的协议类型、源端口、目的端口等5元组信息进行流量匹配。
  - 基于MAC地址ACL4000～4999主要用于对以太网等数据链路层协议帧头中的源MAC地址、目的MAC地址、类型字段等信息进行流量匹配。
  - 硬件包过滤ACL是一种特殊的ACL，将硬件包过滤ACL下发到接口卡上后，接口卡通过硬件实现包过滤功能，比普通的软件包过滤速度更快，消耗系统资源更少。硬件包过滤ACL的匹配条件比较全面，可以通过源IP地址、目的IP地址、源MAC地址、目的MAC地址、协议等维度来进行流量匹配。

在基于基本或高级ACL的接口包过滤中，inbound指接口收到的报文，outbound指接口发送的报文。在基于MAC地址的包过滤中，只支持inbound一个方向，即只对接口收到的报文进行过滤。在硬件包过滤中，只支持inbound一个方向，即只对接口收到的报文进行过滤。

每个接口只能应用一条ACL。如果重复配置，新配置的ACL将覆盖旧的ACL。

- 创建高级ACL，并进入ACL视图

  acl [**number**] *acl-number* [**match-order** { **config** | **auto** }]

- 配置指定协议信息的高级ACL规则

  举例：rule deny tcp source 129.9.0.0 0.0.255.255 destination 202.38.160.0 0.0.0.255 destination-port equal www

- 查看ACL匹配情况

  <USG5000>display ACL 2001

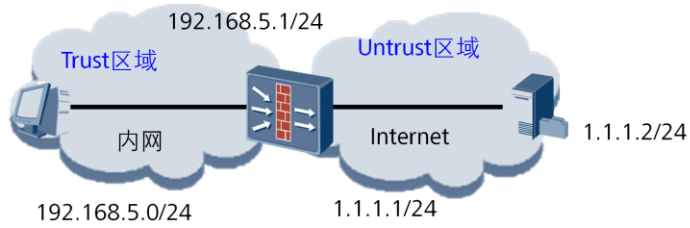
  rule 0 permit source 10.32.255.0 0.0.0.255 （27 times matched）

从例子中可以看出ACL 2001中规则的匹配情况，给故障诊断提供了依据，具体步骤参考故障诊断。

- ACL的应用场景
  - 防火墙接口包过滤应用
  - QoS应用
  - 策略路由应用
  - 路由策略应用
  - IPSec应用

域间转发策略配置举例

- 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。



HUAWEI

配置思路：

1. 规划转发策略。

需求是需要允许192.168.5.0/24这个大范围的网段通过，然后拒绝这个范围内的几个特殊IP。这样需要配置2条转发策略，先配置拒绝特殊IP通过的转发策略，然后再配置允许整个网段通过的转发策略。如果配置反了，几个特殊的IP就会先匹配上大范围的策略通过防火墙了，不会再继续匹配下边的特殊策略了。

2. 地址集规划。

需求中是通过IP地址控制访问权限，那么需要在转发策略中指定IP地址作为匹配条件。对于连续的地址段可以在策略中直接配置，但是对于零散的地址建议配置为地址集，对地址集进行统一控制，而且也方便被其他策略复用。所以在本例中可以将几个特殊的IP地址配置成一个地址集。

3. 配置转发策略，控制上网权限。

关键配置（命令行）

- 创建拒绝特殊的几个IP地址访问Internet的转发策略

  [USG] policy interzone trust untrust outbound

  [USG-policy-interzone-trust-untrust-outbound] policy 0

  [USG-policy-interzone-trust-untrust-outbound-0] policy source address-set ip_deny

  [USG-policy-interzone-trust-untrust-outbound-0] action deny

- 创建允许192.168.5.0/24这个网段访问Internet的转发策略

  [USG-policy-interzone-trust-untrust-outbound] policy 1

  [USG-policy-interzone-trust-untrust-outbound-1] policy source 192.168.5.0 mask 24

  [USG-policy-interzone-trust-untrust-outbound-1] action permit

ip_deny地址集配置如下：

[USG] ip address-set ip_deny type object

[USG-object-address-set-ip_deny] address 192.168.5.2 0

[USG-object-address-set-ip_deny] address 192.168.5.3 0

[USG-object-address-set-ip_deny] address 192.168.5.6 0

Thank you

www.huawei.com