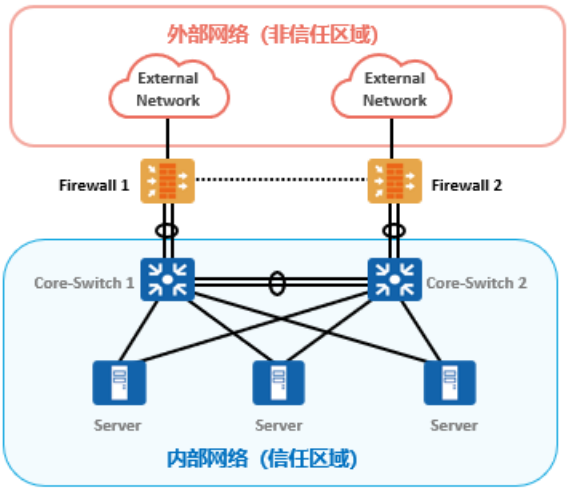
华为防火墙技术

- “防火墙”一词起源于建筑领域，用来隔离火灾，阻止火势从一个区域蔓延到另一个区域。引入到通信领域，防火墙这一具体设备通常用于两个网络之间有针对性的、逻辑意义上的隔离。这种隔离是选择性的，隔离“火”的蔓延，而又保证“人”可以穿墙而过。这里的“火”是指网络中的各种攻击，而“人”是指正常的通信报文。
- 本课程将介绍在通信领域中什么是防火墙，为什么需要防火墙，以及防火墙的基本工作原理和配置。

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
  - 防病毒

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。

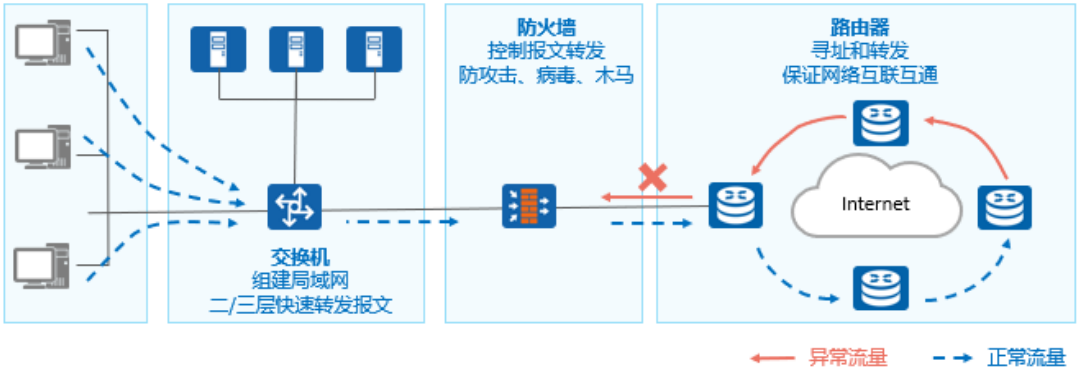
框式防火墙

盒式防火墙

- 严格意义上，防火墙还有更多的部署形态，例如桌面型防火墙（盒式防火墙的一种）。桌面型防火墙适用于小型企业、行业分支、连锁商业机构等场景。华为盒式防火墙同时支持传统模式和云管理模式。云管理模式由云端统一管理分支机构的安全接入，支持设备即插即用、业务配置自动化、运维可视化和网络大数据分析。
- 本课程不过多介绍桌面型防火墙和软件防火墙，后续内容聚焦的框式/盒式硬件防火墙。

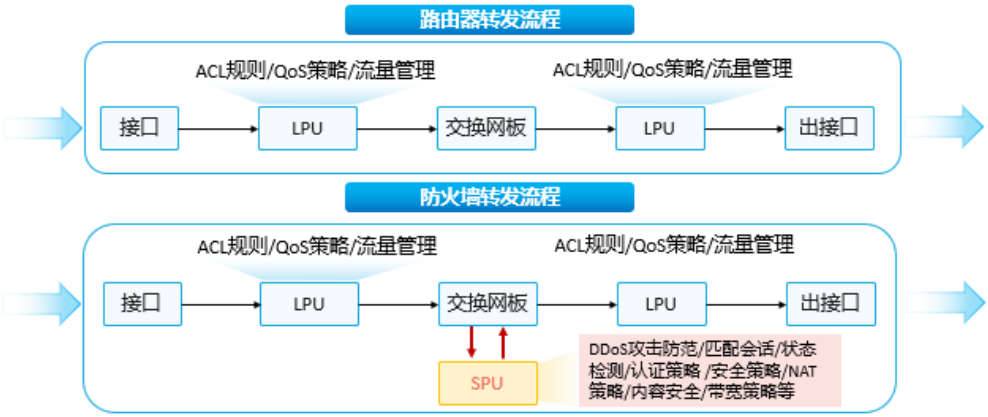
防火墙与交换机、路由器功能对比

- 以园区网为例，交换机作用是接入终端和汇聚内部路由，组建内部互联互通的局域网。
- 路由器作用是路由的分发、寻址和转发，构建外部连接网络。
- 防火墙作用是流量控制和安全防护，区分和隔离不同安全区域。

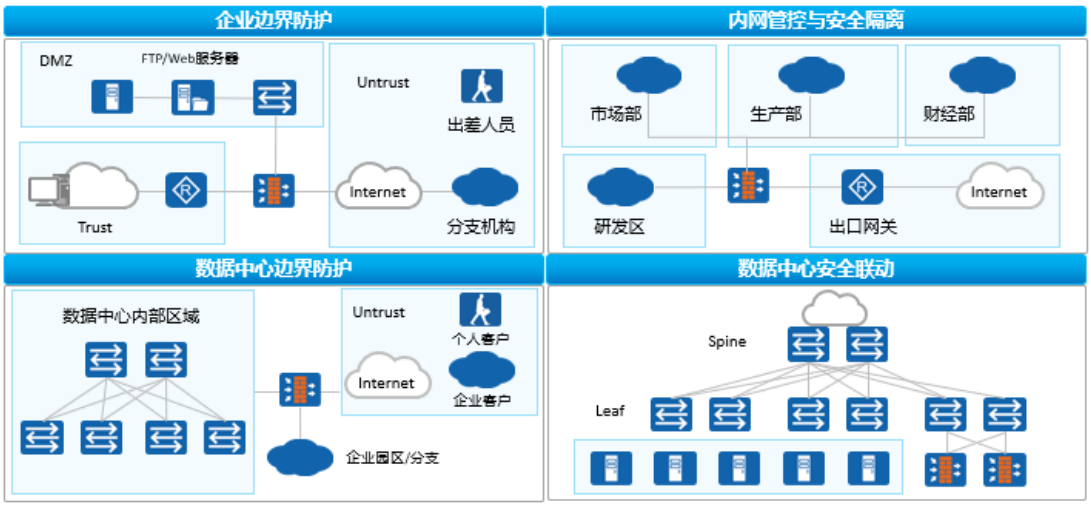


防火墙与路由器转发流程对比

- 防火墙的转发流程比路由器复杂。以框式设备为例，硬件上除了接口、LPU（Line Processing Unit）、交换网板等外，防火墙还特有SPU（Service Processing Unit），用于实现防火墙的安全功能。



防火墙的典型应用场景



- DMZ（Demilitarized Zone）起源于军方，是介于严格的军事管制区和松散的公共区域之间的一种有着部分管制的区域。防火墙设备引用了这一术语，指代一个逻辑上和物理上都与内部网络和外部网络分离的安全区域。在企业中一般用于服务器的放置。
- 数据中心网络一般采用 Spine-Leaf 架构。Spine 为骨干节点负责流量高速转发，Leaf 为叶子节点负责服务器、防火墙或其他设备接入。Spine-Leaf 之间全三层互联。

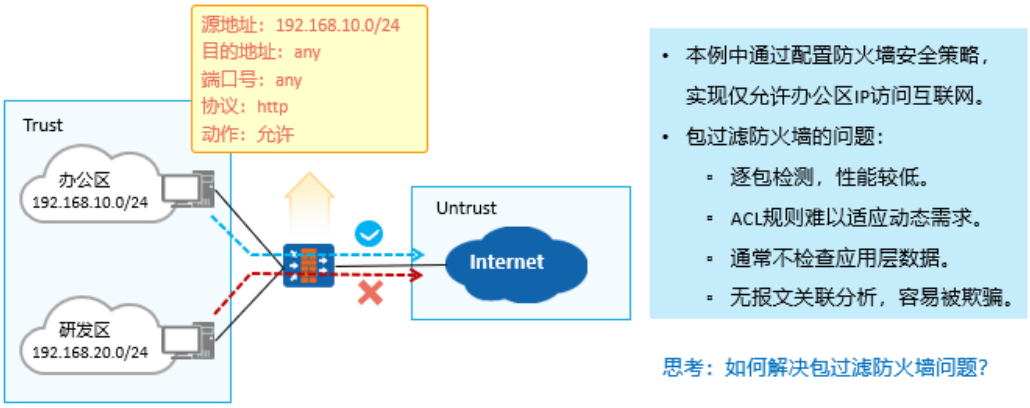
防火墙的发展历程

- 纵观防火墙的发展历史，防火墙经历了从低级到高级、从功能简单到功能复杂的过程。网络技术的不断发展和新需求的不断提出，推动着防火墙的发展。
- 防火墙从包过滤防火墙发展起经历了状态检测、统一威胁管理、NGFW等到AI防火墙，有以下特点：
  - 访问控制越来越精细
  - 防护能力越来越强
  - 性能越来越高

- 更多防火墙发展历史，请参考《强叔侃墙》

包过滤防火墙

- 包过滤是指基于五元组对每个数据包进行检测，根据配置的安全策略转发或丢弃数据包。
- 包过滤防火墙的基本原理是：通过配置访问控制列表（Access Control List，ACL）实施数据包的过滤。

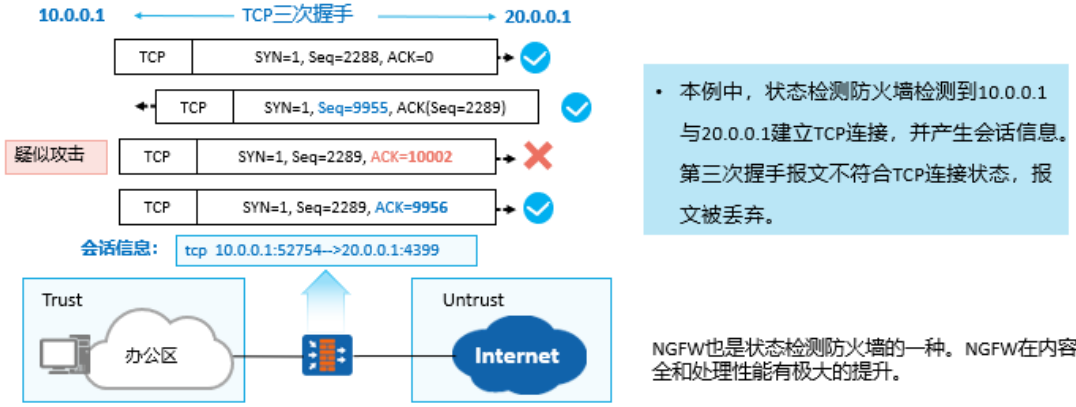


- 包过滤防火墙主要基于数据包中的源/目的 IP 地址、源/目的端口号、IP 标识和报文传递的方向等信息。
- 包过滤防火墙的设计简单，非常易于实现，而且价格便宜。
- 包过滤防火墙的缺点主要表现以下几点：
- 随着 ACL 复杂度和长度的增加，其过滤性能呈指数下降；
- 静态的 ACL 规则难以适应动态的安全要求；
- 包过滤不检查会话状态也不分析数据，这很容易让黑客

蒙混过关。例如，攻击者可以使用假冒地址进行欺骗，通过把自己主机 IP 地址设成一个合法主机 IP 地址，就能很轻易地通过报文过滤器。

状态检测防火墙

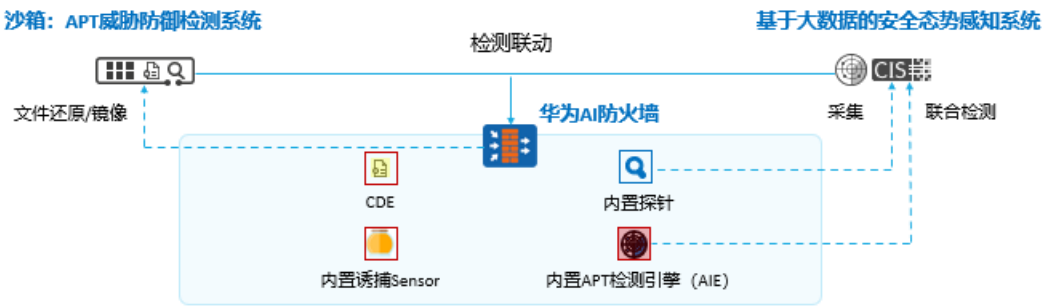
- 状态检测是包过滤技术的发展，它考虑报文前后的关联性，检测的是连接状态而非单个报文。
- 状态检测防火墙就是支持状态检测功能的防火墙。



- 状态检测防火墙通过对连接的首个数据包（后续简称首包）检测而确定一条连接的状态。后续数据包根据所属连接的状态进行控制（转发或阻塞）。

AI防火墙

- AI防火墙是结合AI技术的新一代防火墙。它通过结合AI算法或AI芯片等多种方式，进一步提高了防火墙的安全防护能力和性能。
- 华为AI防火墙，内置的恶意文件检测引擎CDE、诱捕Sensor、APT检测引擎和探针，支持与沙箱和华为大数据分析平台CIS联动检测，打造智能防御体系。



- 华为 HiSecEngine USG6000E 系列是业界首批推出的 AI

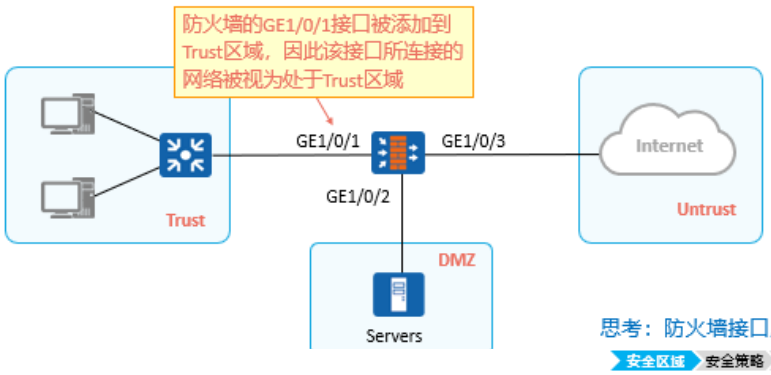
防火墙。AI 防火墙没有统一的标准，例如通过用大量数据和算法“训练”防火墙，让其学会自主识别威胁；通过内置 AI 芯片，提高应用识别和转发性能，都可以被称为 AI 防火墙。

- APT（Advanced Persistent Threat，高级持续性威胁）是指用先进的攻击手段对特定目标进行长期持续性攻击的攻击形式。
- 沙箱（Sandbox）是一个用于检测病毒的安全设备，它为疑似病毒构建虚拟环境，通过观察其后续行为检测病毒。沙箱是 APT 检测的重要设备。华为的沙箱产品为 Firehunter。
- CIS（Cybersecurity Intelligence System）能够对网络中的流量及各类设备的网络、安全日志等海量网络基础数据执行有效采集，通过大数据实时及离线分析，结合机器学习技术、专家信誉、情报驱动，有效的发现网络中的潜在威胁和高级威胁，实现企业内部的全网安全态势感知，同时可以结合华为 HiSec 解决方案高效地完成威胁的处置闭环，防患未然。
- 自研恶意文件检测引擎（CDE）引入 PE Class 2.0 AI 算法，对全文件进行还原，对文件内容进行深度检测。（业界主流基于流检测。流检测的检测速度快，但只还原文件头，不对文件内容进行检查。
- 华为独创的 AIE APT 检测引擎，引入 AI 算法，持续防御最新威胁。
- 更多 AI 防火墙相关内容请参考 https://e.huawei.com/cn/products/enterprise-networking/security 和 https://e.huawei.com/cn/material/networking/e1869bfff9ca42c1b4f6a83f69118215。

安全区域 安全策略 会话表 Server-map

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。

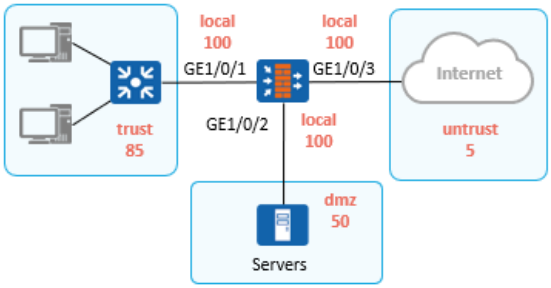


思考：防火墙接口属于安全区域吗？

安全区域 安全策略 会话表 Server-map

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，也不允许修改安全优先级。
  - 每个Zone都必须设置一个安全优先级（Priority），值越大，则Zone的安全优先级越高。
  - 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。

防火墙默认安全区域均为小写字母，且大小写敏感，包括：

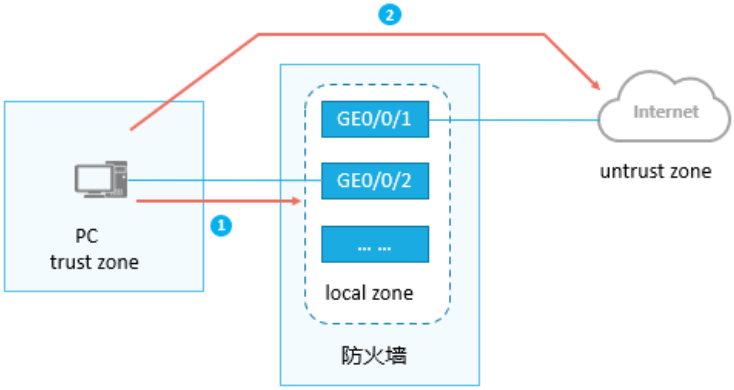
- 非受信区域（untrust）：通常用于定义 Internet 等不安全的网络。
- 非军事化区域（dmz）：通常用于定义内网服务器所在区域。因为这种设备虽然部署在内网，但是经常需要被外网访问，存在较大安全隐患，同时一般又不允许其主动访问外网，所以将其部署一个优先级比 trust 低，但是比 untrust 高的安全区域中。
- DMZ（Demilitarized Zone）起源于军方，是介于严格的

军事管制区和松散的公共区域之间的一种有着部分管制的区域。防火墙设备引用了这一术语，指代一个逻辑上和物理上都与内部网络和外部网络分离的安全区域。

- DMZ 安全区域很好地解决了服务器的放置问题。该安全区域可以放置需要对外提供网络服务的设备，如 WWW 服务器、FTP 服务器等。上述服务器如果放置于内部网络，外部恶意用户则有可能利用某些服务的安全漏洞攻击内部网络；如果放置于外部网络，则无法保障它们的安全。
- 受信区域（trust）：通常用于定义内网终端用户所在区域。
- 本地区域（local）：local 区域定义的是设备本身，包括设备的各接口本身。凡是由设备构造并主动发出的报文均可认为是从 Local 区域中发出，凡是需要设备响应并处理（而不仅是检测或直接转发）的报文均可认为是由 local 区域接收。用户不能改变 local 区域本身的任何配置，包括向其中添加接口。
- 由于 local 区域的特殊性，在很多需要设备本身进行报文收发的应用中，需要开放对端所在安全区域与 local 区域之间的安全策略。

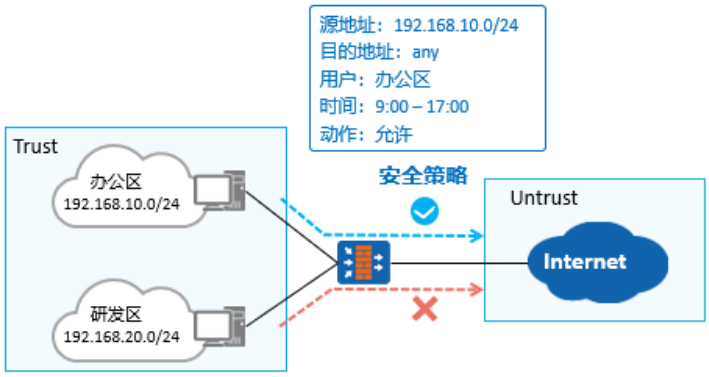
区域间（Interzone）示例

- 流量的源、目的地址决定了互访的区域。本例1中PC访问防火墙的接口的流量实际上是从trust zone到达local zone；本例2中PC访问Internet的流量实际上是从trust zone到达untrust zone。



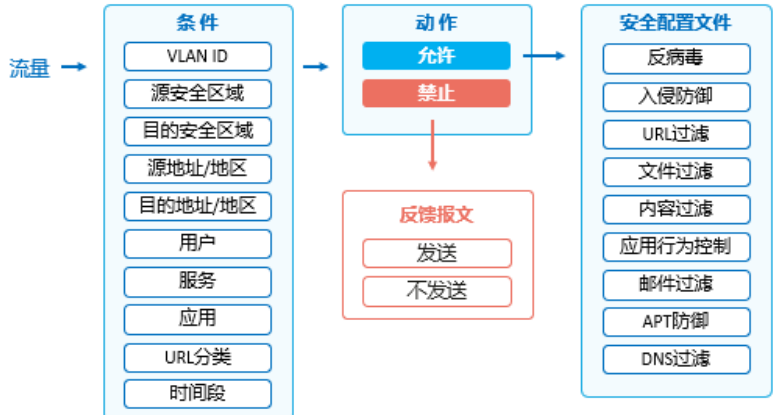
防火墙基本概念：安全策略

- 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。



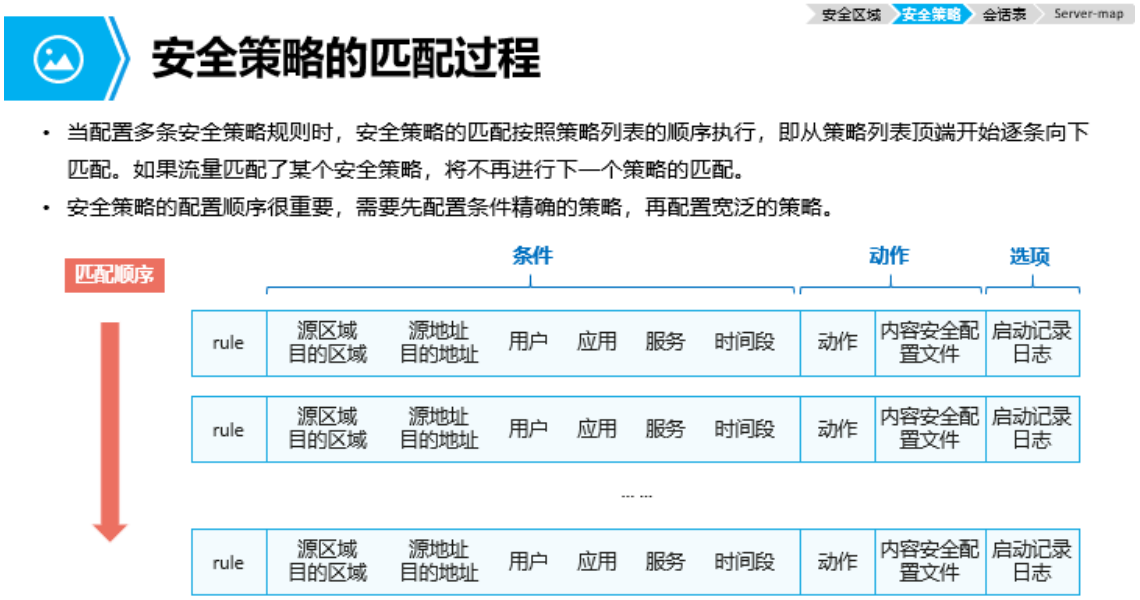
安全策略组成

- 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。

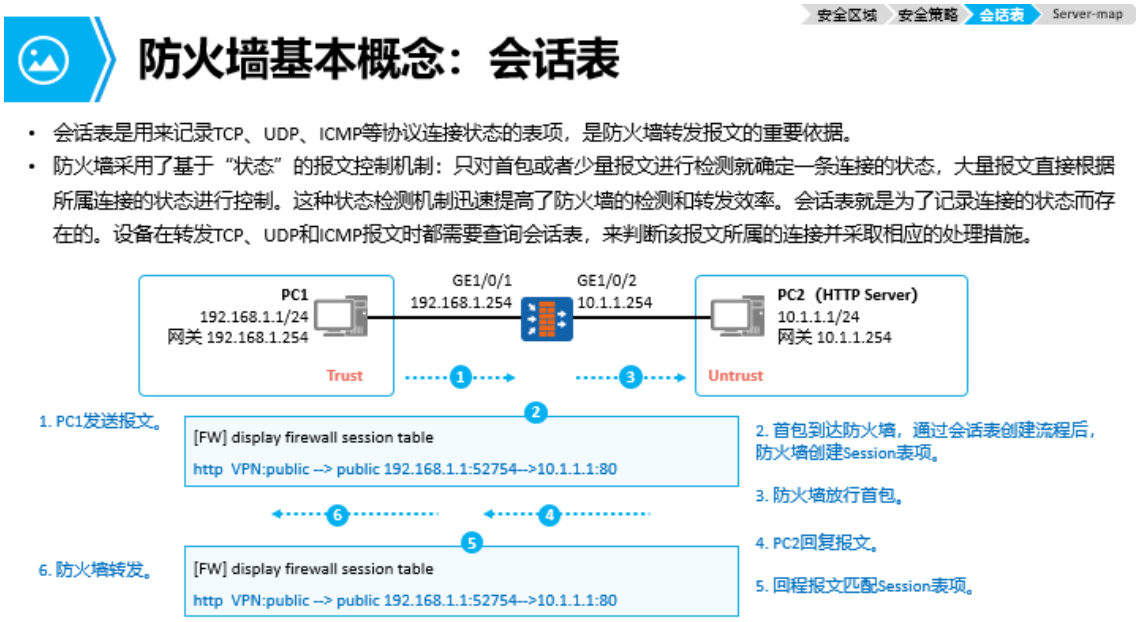


- 动作说明：
- 允许：如果动作为“允许”，则对流量进行如下处理：
- 如果没有配置内容安全检测，则允许流量通过。
- 如果配置内容安全检测，最终根据内容安全检测的结论来判断是否对流量进行放行。内容安全检测包括反病毒、入侵防御等，它是通过在安全策略中引用安全配置文件实现的。如果其中一个安全配置文件阻断该流量，则防火墙阻断该流量。如果所有的安全配置文件都允许该流量转发，则防火墙允许该流量转发。
- 禁止：表示拒绝符合条件的流量通过。
- 如果动作为“禁止”，防火墙不仅可以将报文丢弃，还可以针对不同的报文类型选择发送对应的反馈报文。发起连接请求的客户端/服务器收到防火墙发送的阻断报文后，可以快速结束会话并让用户感知到请求被阻断。
- Reset 客户端：防火墙向 TCP 客户端发送 TCP reset 报文。
- Reset 服务器：防火墙向 TCP 服务器发送 TCP reset 报文。
- ICMP 不可达：FW 向报文客户端发送 ICMP 不可达报文。

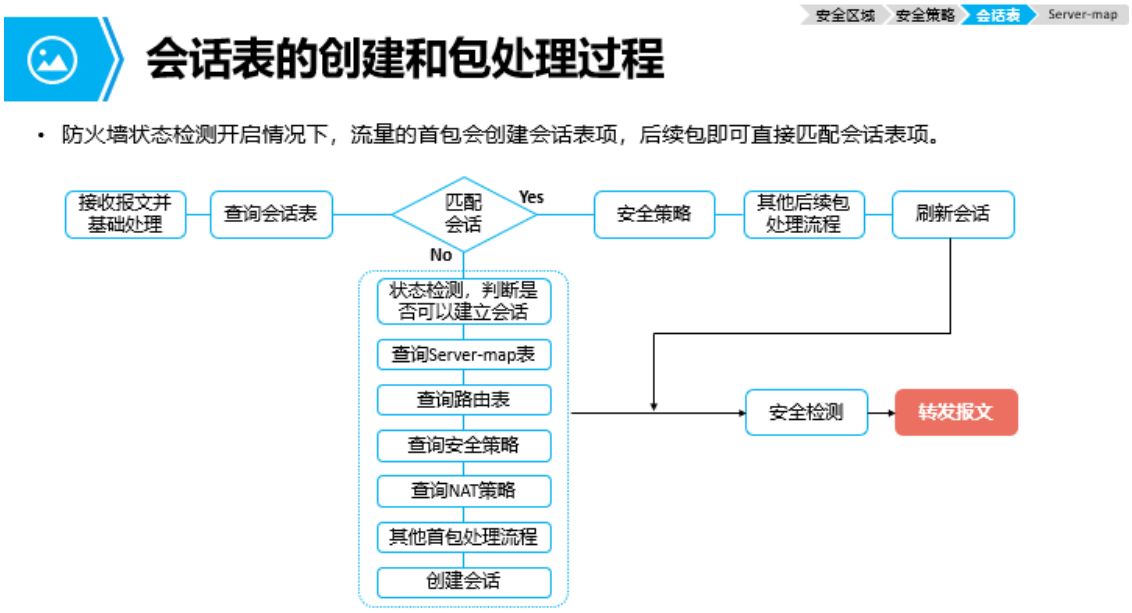
- 更多详细信息，可以参考文档，“安全策略”章节，https://support.huawei.com/hedex/hdx.do?docid=EDOC1100084128&lang=zh&idPath=24030814%7C9856724%7C21430823%7C22984765%7C23176238。



- 系统默认存在一条缺省安全策略 default。缺省安全策略位于策略列表的最底部，优先级最低，所有匹配条件均为 any，动作默认为禁止。如果所有配置的策略都未匹配，则将匹配缺省安全策略 default。



- 本例中 PC1 向 PC2 发起 HTTP 连接，所以在防火墙会话表中标示出“http”协议和连接信息，并识别出此流量在公共路由表中被转发（图中 VPN:public）。



- 本流程只是一个示意图，展示了华为防火墙各个模块的基本处理顺序。实际不同的报文处理并非严格按照此流程图依次进行（若无对应配置），且与具体产品实现相关。
- 更多详细信息，可以参考指定型号防火墙产品文档，“报文转发流程”章节。

会话表的老化时间与长连接

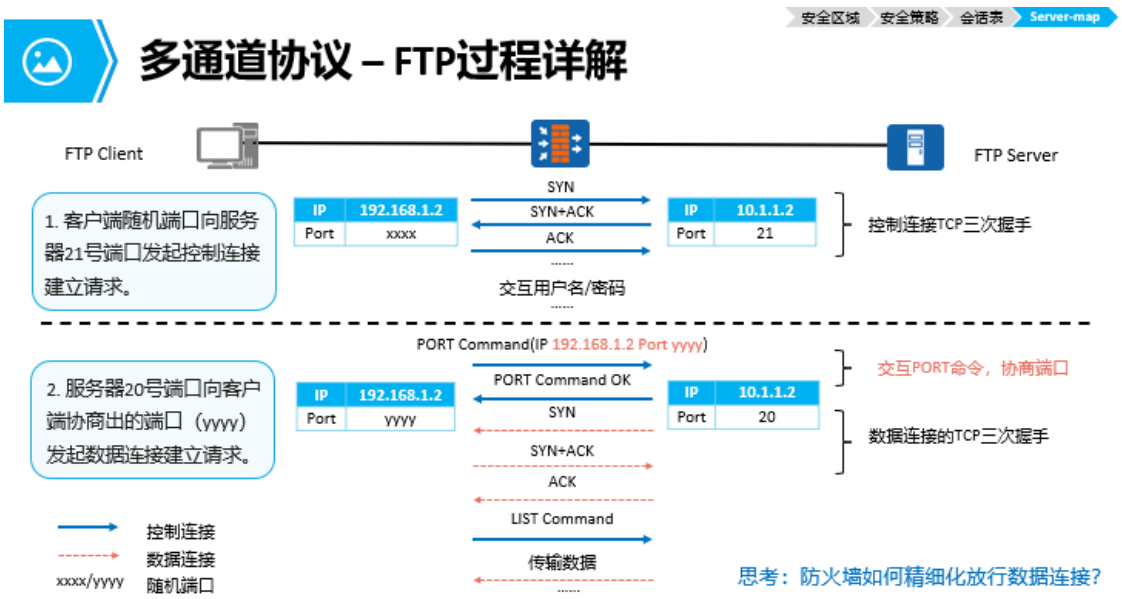
- 防火墙为各种协议设定了会话老化机制。当一条会话在老化时间内没有被任何报文匹配，则会被从会话表中删除。这种机制可以避免防火墙的设备资源被大量无用、陈旧的会话表项消耗。
- 但是对于某些特殊业务中，一条会话的两个连续报文可能间隔时间很长。例如：
- 用户通过 FTP 下载大文件，需要间隔很长时间才会在控制通道继续发送控制报文。
- 用户需要查询数据库服务器上的数据，这些查询操作的

时间间隔远大于 TCP 的会话老化时间。

- 此时如果其会话表项被删除，则该业务会中断。长连接（Long Link）机制可以给部分连接设定超长的老化时间，有效解决这个问题。

- 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。
- FTP 协议是一个典型的多通道协议，在其工作过程中，FTP Client 和 FTP Server 之间将会建立两条连接：控制连接和数据连接。控制连接用来传输 FTP 指令和参数，其中就包括建立数据连接所需要的信息。数据连接用来获取服务器目录及传输数据。数据连接使用的端口号是在控制连接中临时协商的。根据数据连接的发起方式 FTP 协议分为两种工作模式：主动模式（PORT 模式）和被动模式（PASV 模式）。主动模式中，FTP Server 20 号端口主动向 FTP Client 随机端口发起数据连接；被动模式中，FTP Server 被动接收 FTP Client 发起的数据连接。模式在一般的 FTP 客户端中都是可以设置的，这里我们以主动模式为例。

- 多通道协议存在时，防火墙配置较为宽泛的安全策略也可以解决协议不可用问题，但是存在安全隐患。

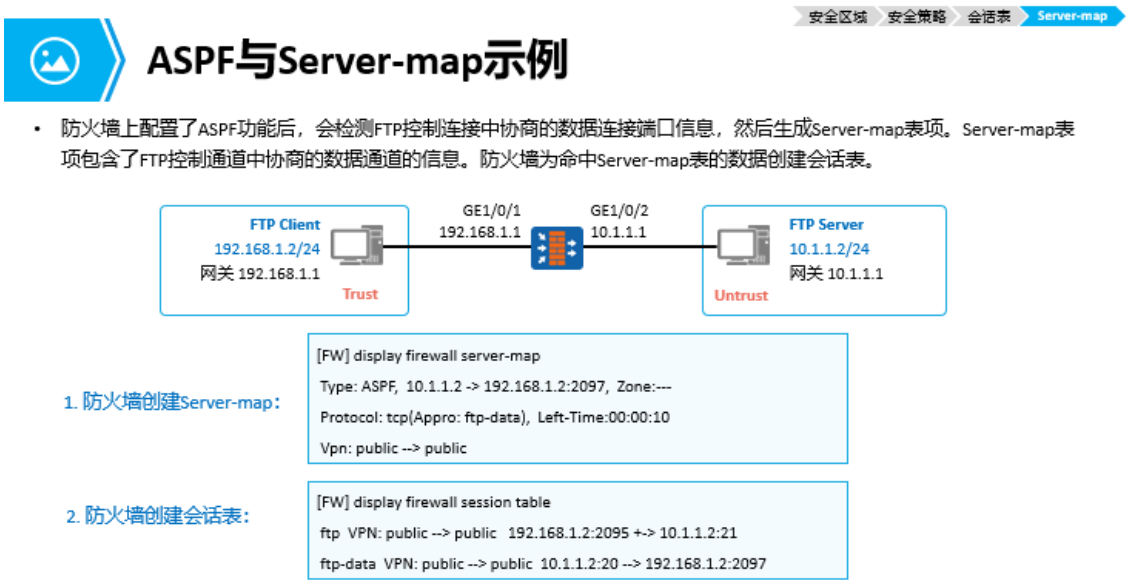


- 大部分多媒体应用协议（如 H.323、SIP）、FTP、netmeeting 等协议使用约定的固定端口来初始化一个控制连接，再动态的协商出端口用于数据传输。端口的选择是不可预测的。其中的某些应用甚至可能要同时用到多个端口。传统的包过滤防火墙可以通过配置 ACL 过滤规则匹配单通道协议的应用传输，保障内部网络不受攻击，但只能阻止一些使用固定端口的应用，无法匹配使用协商出随机端口传输数据的多通道协议应用，留下了许多安全隐患。

ASPF 与 Server-map

- 为了解决多通道协议的问题，防火墙需要识别协议在应用层协商的地址和端口。这需要开启 ASPF（Application Specific Packet Filter，针对应用层的包过滤）功能。
- ASPF 也称作基于状态的报文过滤，ASPF 功能可以自动检测某些报文的应用层信息并根据应用层信息放开相应的访问规则，即生成 Server-map 表。

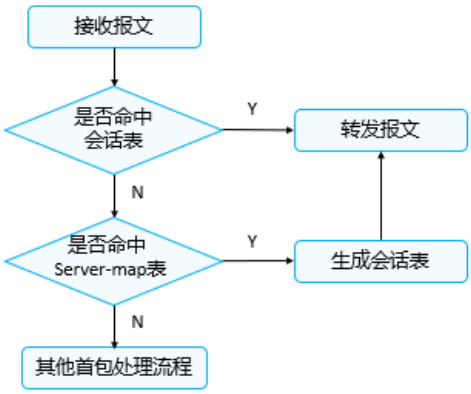
- Server-map 表也记录了类似会话表中连接的状态。Server-map 表中的信息相对简单，是简化的会话表，在真实流量到达前生成。在流量真实到达防火墙时，防火墙会基于 Server-map 表生成会话表，然后执行转发。
- 开启 ASPF 解决多通道协议问题，是生成 Server-map 表的一种方式。



- Server-map 表与会话表的关系如下：
- Server-map 表记录了应用层数据中的关键信息，报文命中该表后，不再受安全策略的控制；
- 会话表是通信双方连接状态的具体体现；
- Server-map 表不是当前的连接信息，而是防火墙对当前连接分析后得到的即将到来报文的预测；
- 防火墙收到报文先检查是否命中会话表；
- 如果没有命中则检查是否命中 Server-map 表；
- 命中 Server-map 表的报文不受安全策略控制；
- 防火墙最后为命中 Server-map 表的数据创建会话表。

Server-map表与简化的包转发过程

- 当防火墙接收到一个报文且没有命中会话表时，防火墙进入首包处理流程，查询是否有命中的Server-map表。如果有，则会生成会话表转发报文；如果没有，则执行其他包处理过程。



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。

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本地防火墙。

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
```

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-zone-name] add interface interface-type { interface-number | interface-number.subinterface-number }
```

安全区域在使用时需要与防火墙的特定接口相关联，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**

   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) 创建规则

   [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** *}*

   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}*

   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}*

   命令中mask-address使用反掩码。

7. (安全策略规则视图) 配置服务

   [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动作

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

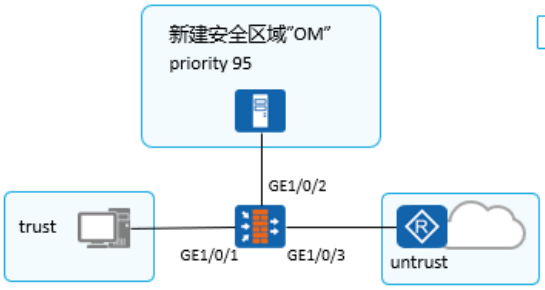
   防火墙默认的动作为**deny**。

- 安全策略规则视图中指定源、目的 IP 地址可以有很多的可选参数，例如 IP 地址组、地区和地区组等，本课程不做过多介绍。更多详细内容请参考产品文档。

防火墙配置案例

案例描述：

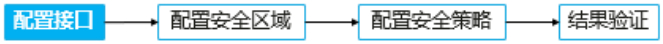
- 防火墙将网络隔离为三个安全区域，trust、untrust和OM，其中OM区域优先级为95。现有需求如下：
  - 允许防火墙接口GE1/0/1响应Ping请求。
  - 允许OM区域ICMP流量访问untrust区域。



配置过程分为四个步骤：

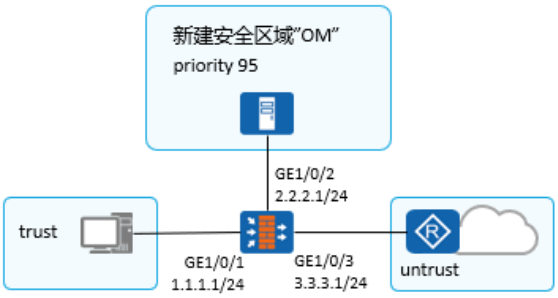
- 配置防火墙接口。
- 配置防火墙安全区域。
- 配置防火墙安全策略。
- 结果验证。

配置案例 - 接口



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。



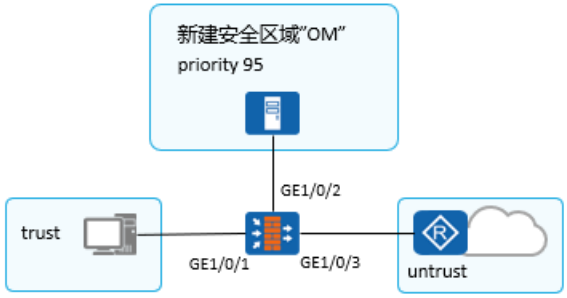

```
#配置接口IP地址并允许GE1/0/1的ping业务
[FW] interface GigabitEthernet 1/0/1
[FW-GigabitEthernet1/0/1] ip address 1.1.1.1 24
[FW-GigabitEthernet1/0/1] service-manage ping permit
[FW-GigabitEthernet1/0/1] interface GigabitEthernet 1/0/2
[FW-GigabitEthernet1/0/2] ip address 2.2.2.1 24
[FW-GigabitEthernet1/0/2]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



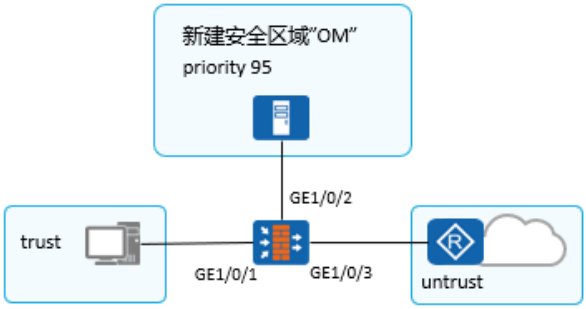

```
#创建安全区域
[FW] firewall zone name OM
[FW-zone-OM] set priority 95
[FW-zone-OM] quit

#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。

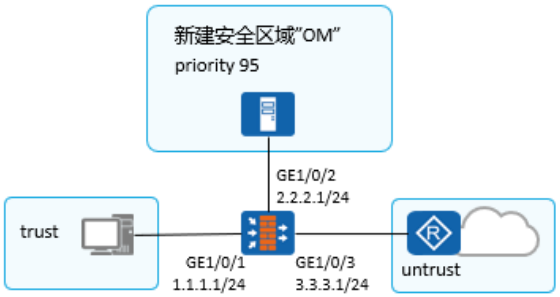



```
#创建安全策略
[FW-policy-security] rule name R1
[FW-policy-security-rule-R1] source-zone OM
[FW-policy-security-rule-R1] destination-zone untrust
[FW-policy-security-rule-R1] service icmp
[FW-policy-security-rule-R1] action permit
```

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。

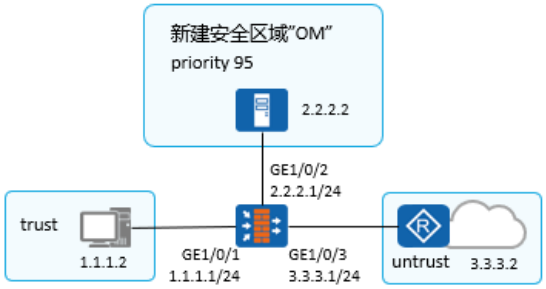



```
#查看防火墙会话表
[FW]display firewall session table
2020-03-11 10:31:21.010
 Current Total Sessions : 4
 icmp  VPN: public --> public  1.1.1.2:14265 --> 1.1.1.1:2048
 icmp  VPN: public --> public  1.1.1.2:15289 --> 1.1.1.1:2048
 icmp  VPN: public --> public  1.1.1.2:14777 --> 1.1.1.1:2048
 icmp  VPN: public --> 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. OM区域2.2.2.2向untrust区域3.3.3.2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  2.2.2.2:63928 --> 3.3.3.2:2048
 icmp  VPN: public --> public  2.2.2.2:63672 --> 3.3.3.2:2048
 icmp  VPN: public --> public  2.2.2.2:63416 --> 3.3.3.2:2048
 icmp  VPN: public --> public  2.2.2.2:62904 --> 3.3.3.2:2048
```

思考：ICMP没有端口，这里防火墙会话表中的端口号是?

- ICMP 没有端口，但是防火墙在生成 ICMP 流量对应的会话表时会生成相应的端口号以满足状态检测。

思考题：

- （单选题）缺省情况下，防火墙有几个安全区域？（ ）

  A. 1　　B. 2　　C. 3　　D. 4
- （判断题）防火墙在生产会话表之前，都需要先生成 Server-map。（ ）
- （多选题）以下对于华为 AI 防火墙说法正确的是？（

)

A. 内置恶意文件检测引擎（CDE)
B. 内置探针
C. 内置 APT 检测引擎（AIE）
D. 内置独创诱捕 Sensor

答案：

- D
- F
- ABCD
-