- 1. 防火墙
  - 1.1 四个基本安全区域
  - 1.2 域间数据流方向
  - 1.3 区域策略
  - 1.4 防火墙配置
    - 1 配置ip地址
    - 2 配置区域
    - 3 把接口加入区域中
    - 4 在区域间应用访问控制列表
  - 防火墙访问控制

1. 防火墙

1.1 四个基本安全区域

防火墙的安全区域

防火墙的内部划分为多个区域，所有的转发接口都唯一的属于某个区域

华为防火墙上保留四个安全区域：
非受信区（Untrust）：低级的安全区域，其安全优先级为5。
非军事化区（DMZ）：中度级别的安全区域，其安全优先级为50。
受信区（Trust）：较高级别的安全区域，其安全优先级为85。
本地区域（Local）：最高级别的安全区域，其安全优先级为100。
此外，如认为有必要，用户还可以自行设置新的安全区域并定义其安全优先级别。最多16个安全区域。

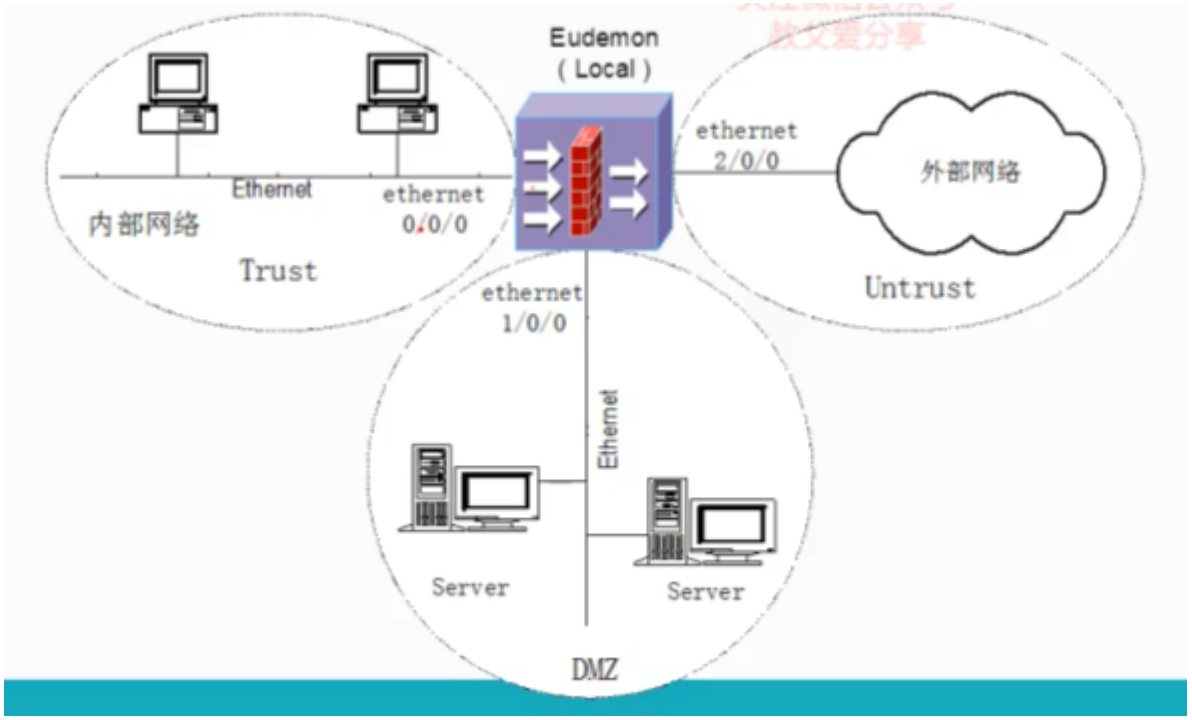
1.2 域间数据流方向

方向以双方第一个出流量的方向定义

域间的数据流分两个方向：
入方向（inbound）：数据由低级别的安全区域向高级别的安全区域传输的方向；
出方向（outbound）：数据由高级别的安全区域向低级别的安全区域传输的方向。

1.3 区域策略

本域内不同接口间不过滤直接转发
进、出接口相同的报文被丢弃
接口没有加入域之前不能转发包文



1.4 防火墙配置

1 配置ip地址

配置IP地址，把各接口的IP地址配置好

配置防火墙接口Ethernet 0/0/0。
[Eudemon] interface ethernet 0/0/0
[Eudemon-Ethernet0/0/0] ip address 192.168.1.1 255.255.255.0
如为双机，需要在接口下配置vrrp
[Eudemon]int eth 0/0/0
[Eudemon-ethernet0/0/0]ip address 192.168.10.1 255.255.255.0
在接口eth0/0/0下配置VRRP备份组1，注意虚拟IP需要和接口地址同一网段
[Eudemon-ethernet0/0/0]vrrp vrid 1 virtual-ip 192.168.10.4
[Eudemon-ethernet0/0/0]interface ethernet 0/0/1
[Eudemon-ethernet0/0/1]ip address 192.168.3.1 255.255.255.0
在接口eth0/0/1下配置VRRP备份组2
注意：在接口下配置vrrp时，不要配置vrrp优先级

2 配置区域

配置区域

配置区域，并把区域优先级配置好（采用缺省区域则不用）
#配置区域dmz。
[Eudemon] firewall zone name dmz1
[Eudemon-zone-dmz1] set priority 70

3 把接口加入区域中

把相应的接口加入到相应的区域中去
配置接口Ethernet 1/0/0加入防火墙DMZ域。
[Eudemon] firewall zone dmz
[Eudemon-zone-dmz] add interface ethernet 1/0/0
[Eudemon-zone-dmz] quit

4 在区域间应用访问控制列表

例子：创建编号为3001的访问控制列表。

```
[华为] acl number 3001
# 配置ACL规则，允许特定用户从外部网访问内部服务器。
[华为-acl-adv-3001] rule permit tcp source 202.39.2.3 0 destination 129.38.1.1 0
[华为-acl-adv-3001] rule permit tcp source 202.39.2.3 0 destination 129.38.1.2 0
[华为-acl-adv-3001] rule permit tcp source 202.39.2.3 0 destination 129.38.1.3 0
下面的配置是在包过滤应用中引用ACL，相关命令的具体解释请见相关章节的描述。
# 将ACL规则3000作用于Trust区域到Untrust区域间的出方向。
[华为-Interzone-trust-untrust] packet-filter 3000 outbound
# 将ACL规则3001作用于Trust区域到Untrust区域间的入方向。
[华为-Interzone-trust-untrust] packet-filter 3001 inbound
# 在Trust区域和Untrust区域之间使能FTP协议的应用协议检测。
[华为-Interzone-trust-untrust] detect ftp
```

进入域间 firewall interzone x y

```
# 将ACL规则3001作用于Trust区域到Untrust区域间的出方向。
[Eudemon]firewall interzone trunst untrust
[Eudemon -Interzone-trust-untrust] packet-filter 3000 outbound
# 将ACL规则3001作用于Trust区域到Untrust区域间的入方向。
[Eudemon -Interzone-trust-untrust] packet-filter 3001 inbound
# 在Trust区域和Untrust区域之间使能FTP协议的应用协议检测。
[Eudemon -Interzone-trust-untrust] detect ftp
```

防火墙访问控制