**实验二、配置通过包过滤实现基本访问控制**

安全区域和包过滤是最基本的防火墙功能，可以用来实现最简单的访问控制功能。本实验将使用路由口，实现通过安全区域和包过滤控制不同主机访问网络的行为。

**前提条件**

本实验主要关注安全区域与包过滤的配置，关于设备如何接入互联网，以及如何使用NAT功能实现内网主机通过有限的公网IP访问互联网。

**组网需求**

USG部署在某公司的出口，公司内的网络设备主要分为员工PC和服务器两种。希望对员工的访问网络的权限进行差异化管理，有如下需求：

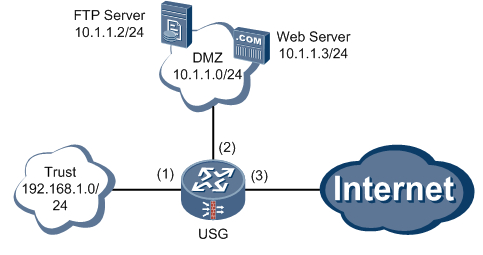
* 部分特殊员工可以拥有访问外部Internet的权限。
* 除特殊员工外的所有员工不能访问Internet。
* 员工之间都可以相互访问。
* 所有员工都可以访问公司的所有服务器。
* Internet网络上任何主机都可以访问公司的FTP服务器和Web服务器。

基于以上几个需求，可以对网络进行如下规划：

* 将所有员工放在同一个安全区域，不对这些员工之间的互访进行监控。
* 将所有服务器放在另外一个安全区域，以避免外网用户通过服务器中转对内网用户进行攻击。
* 配置ACL划定特殊员工，以给这些员工专门开启访问Internet的权限。

最终组网图如图1所示。

**图1** 配置通过包过滤实现基本访问控制组网图



| **项目** | **数据** | **说明** |
| --- | --- | --- |
| (1) | 接口号：GigabitEthernet 0/0/2  IP地址：192.168.1.1/24  安全区域：Trust | 该接口通过交换机与员工PC相连，位于同一网段。 |
| (2) | 接口号：GigabitEthernet 0/0/3  IP地址：10.1.1.1/24  安全区域：DMZ | 该接口通过交换机与服务器相连，位于同一网段。 |
| (3) | 接口号：GigabitEthernet 0/0/4  IP地址：1.1.1.1/24  安全区域：Untrust | 该接口与外网相连。此时已经可以接入互联网。 |
| Trust | 地址范围：192.168.1.0/24 | 将所有员工PC部署在Trust区域。 |
| DMZ | 地址范围：10.1.1.0/24  其中部署多个服务器，但是只有两个服务器对外网提供服务：   * FTP服务器：10.1.1.2/24 * Web服务器：10.1.1.3/24 | 将所有服务器的IP地址划为这个网段，并且部署在DMZ区域。 |
| Untrust | 公网地址 | 用于定义外网主机和服务器。 |
| 特殊员工 | 地址范围：192.168.1.10/24～192.168.1.100/24 | 特殊员工可以访问互联网。 |
| 设备管理员 | 地址：192.168.1.2/24 | 设备管理员位于Trust区域，但是其可以登录设备进行配置。 |

**操作步骤**

1. 打开所有域间缺省包过滤，以保证配置过程中业务不会中断。

说明：

 配置包过滤的整体原则：先打开所有域间的缺省包过滤，保证网络通信正常，然后根据需求配置相应域间的严格包过滤，再检查配置是否正确，最后根据网络情况逐个关闭不需要开放的域间缺省包过滤。

<USG> **system-view**

[USG] **firewall packet-filter default permit all**

配置各个接口的IP，并划入相应的安全区域。

[USG] **interface GigabitEthernet 0/0/2**

[USG-GigabitEthernet0/0/2] **ip address 192.168.1.1 24**

[USG-GigabitEthernet0/0/2] **quit**

[USG] **interface GigabitEthernet 0/0/3**

[USG-GigabitEthernet0/0/3] **ip address 10.1.1.1 24**

[USG-GigabitEthernet0/0/3] **quit**

[USG] **interface GigabitEthernet 0/0/4**

[USG-GigabitEthernet0/0/4] **ip address 1.1.1.1 24**

[USG-GigabitEthernet0/0/4] **quit**

[USG] **firewall zone trust**

[USG-zone-trust] **add interface GigabitEthernet 0/0/2**

[USG-zone-trust] **quit**

[USG] **firewall zone dmz**

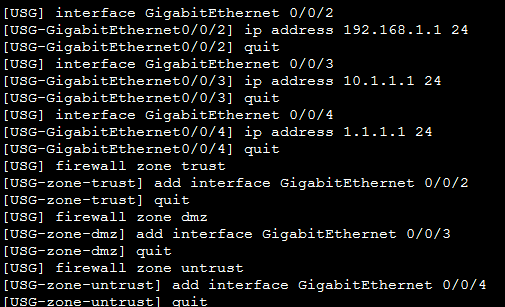
[USG-zone-dmz] **add interface GigabitEthernet 0/0/3**

[USG-zone-dmz] **quit**

[USG] **firewall zone untrust**

[USG-zone-untrust] **add interface GigabitEthernet 0/0/4**

[USG-zone-untrust] **quit**



1. 将Trust区域和DMZ区域之间的缺省包过滤规则改为缺省允许。使得所有员工都能直接访问DMZ区域内的所有服务器。

[USG] **firewall packet-filter default permit interzone trust dmz**



此处没有限定包过滤的方向，则inbound和outbound两个方向的缺省包过滤规则都改为允许。

1. 配置一条Trust与Local域之间的policy用于定义设备管理员访问USG的流量，使设备管理员可以远程登录设备进行配置。

[USG] **policy interzone trust local inbound**

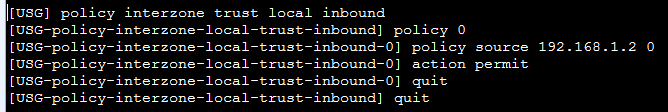
[USG-policy-interzone-local-trust-inbound] **policy 0**

[USG-policy-interzone-local-trust-inbound-0] **policy source 192.168.1.2 0**

[USG-policy-interzone-local-trust-inbound-0] **action permit**

[USG-policy-interzone-local-trust-inbound-0] **quit**

[USG-policy-interzone-local-trust-inbound] **quit**



包过滤方向选为**inbound**是因为管理员所在Trust安全区域的优先级比Local低，如果希望从Trust区域主动访问Local区域，需要选为**inbound**。

1. 配置一个地址集s\_employee用于定于特殊员工的IP地址范围，再创建一条trust和untrust域间的policy允许该部分员工访问untrust区域，完成对特殊员工的放行。

[USG] **ip address-set s\_employee type object**

[USG-object-address-set-s\_employee] **address range 192.168.1.10 192.168.1.100**

[USG-object-address-set-s\_employee] **quit**

[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 s\_employee**

[USG-policy-interzone-trust-untrust-outbound-0] **action permit**

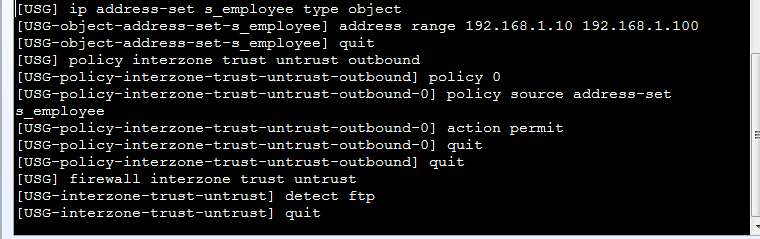
[USG-policy-interzone-trust-untrust-outbound-0] **quit**

[USG-policy-interzone-trust-untrust-outbound] **quit**

[USG] **firewall interzone trust untrust**

[USG-interzone-trust-untrust] **detect ftp**

[USG-interzone-trust-untrust] **quit**



包过滤的方向选为**outbound**可以使Untrust区域内的主机不能主动向Trust区域发起连接。

在Trust和untrust域间应用**detect**命令是为了使内网用户能够正常访问外网中的FTP服务。

1. 配置一个自定义服务集ftp1及其会话老化时间，用于控制通过端口10001访问FTP服务器的流量。同时也可以采用系统预定的ftp服务集，即可省略该步骤。

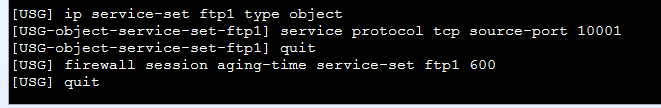
[USG] **ip service-set ftp1 type object**

[USG-object-service-set-ftp1] **service protocol tcp source-port 10001**

[USG-object-service-set-ftp1] **quit**

[USG] **firewall session aging-time service-set ftp1 600**

[USG] **quit**



1. 配置一条DMZ和untrust域间的policy允许Untrust区域的任意主机访问DMZ区域的两个服务器。

规则中只限制报文的目的地址，这样可以保证任意主机都能访问。同时由于限定了目的地址，所以外网主机也只能访问这两个服务器，而不能访问DMZ区域内的其他服务器。这就是为什么不直接将Untrust和DMZ区域的缺省包过滤改为允许，而使用policy放行的原因。

注意：

在使用NAT的情况下，以下命令中应该限定的是NAT转换前的IP地址。例如通过NAT Server功能将10.1.1.2和10.1.1.3分别映射为外网的1.1.1.2、1.1.1.3，则policy应定义为**policy destination range 1.1.1.2 1.1.1.3**。

[USG] **policy interzone dmz untrust inbound**

[USG-policy-interzone-dmz-untrust-inbound] **policy 0**

[USG-policy-interzone-dmz-untrust-inbound-0] **policy destination 10.1.1.2 0**

[USG-policy-interzone-dmz-untrust-inbound-0] **policy service service-set ftp1**

[USG-policy-interzone-dmz-untrust-inbound-0] **action permit**

[USG-policy-interzone-dmz-untrust-inbound-0] **quit**

[USG-policy-interzone-dmz-untrust-inbound] **policy 1**

[USG-policy-interzone-dmz-untrust-inbound-1] **policy destination 10.1.1.3 0**

[USG-policy-interzone-dmz-untrust-inbound-1] **policy service service-set http**

[USG-policy-interzone-dmz-untrust-inbound-1] **action permit**

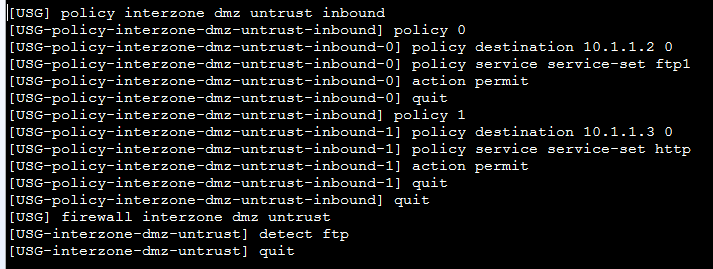
[USG-policy-interzone-dmz-untrust-inbound-1] **quit**

[USG-policy-interzone-dmz-untrust-inbound] **quit**

[USG] **firewall interzone dmz untrust**

[USG-interzone-dmz-untrust] **detect ftp**

[USG-interzone-dmz-untrust] **quit**



在DMZ和untrust域间不同策略中应用**policy service service-set ftp1**和**policy service service-set http**，配置FTP和HTTP服务，允许对应的FTP和HTTP数据通过。

在DMZ和untrust域间应用一条**detect**命令是为了使服务器能够正常对外提供FTP服务。HTTP协议服务默认开启

1. 请根据网络情况逐个关闭不需要开放的域间缺省包过滤。在逐个关闭期间，请关注网络是否能够正常通信。如果在关闭某个域间后影响正常业务，请重新打开该域间的缺省包过滤并检查和修改包过滤的配置。

[USG] **firewall packet-filter default deny interzone local trust**

[USG] **firewall packet-filter default deny interzone trust untrust**

[USG] **firewall packet-filter default deny interzone dmz untrust**







**操作结果**

完成本举例后，可以通过以下操作验证配置是否成功：

1. 为管理员的主机配置静态IP地址192.168.1.2，使用管理员PC ping设备内网接口IP地址192.168.1.1/24。
   1. 如果可以ping通，说明Trust至Local区域的包过滤配置成功。
   2. 如果不能ping通，请依次检查设备与内网主机之间的链路连通性、设备内网接口的IP地址和安全区域配置、Trust区域与Local区域间的包过滤规则。

如果管理员PC可以ping通设备内网接口，说明内网环境没有问题。可以进行下一步验证。

1. 为内网特殊员工PC配置静态IP地址和缺省网关后，访问Internet上的网站。如果可以访问成功，说明Trust区域至Untrust区域的包过滤配置成功。如果不能，可能是设备尚未成功接入互联网、NAT配置有误或上行接口的IP地址、安全区域配置问题。
2. 为内网普通员工PC配置静态IP地址后，访问公司服务器。如果可以访问成功，说明Trust区域至DMZ区域的包过滤配置成功。如果不能，请依次检查DMZ区域的链路连通性、DMZ区域接口的IP地址和安全区域配置以及服务器是否正常提供服务。
3. 从外网访问公司服务器，如果可以访问成功，说明DMZ区域和Untrust区域的包过滤配置成功。如果不能，请依次检查设备是否成功接入互联网、外网接口的IP地址和安全区域配置、DMZ和Untrust区域之间的包过滤配置。同时使用NAT功能的情况下，还需要检查NAT功能是否正确配置以及是否配置了ASPF功能。

**配置脚本**

以下仅给出与本案例有关的脚本。

# sysname USG

# firewall packet-filter default permit interzone trust dmz direction inbound firewall packet-filter default permit interzone trust dmz direction outbound firewall packet-filter default permit interzone local dmz direction inbound firewall packet-filter default permit interzone local dmz direction outbound firewall packet-filter default permit interzone local untrust direction inbound firewall packet-filter default permit interzone local untrust direction outbound

#interface GigabitEthernet0/0/2 ip address 192.168.1.1 255.255.255.0

#interface GigabitEthernet0/0/3 ip address 10.1.1.1 255.255.255.0

#interface GigabitEthernet0/0/4 ip address 1.1.1.1 255.255.255.0

# firewall zone local set priority 100

#firewall zone trust set priority 85 add interface GigabitEthernet0/0/2

#firewall zone untrust set priority 5 add interface GigabitEthernet0/0/4

#firewall zone dmz set priority 50 add interface GigabitEthernet0/0/3

#firewall interzone local trust

#firewall interzzne trust untrust detect ftp

#firewall interzone dmz untrust detect ftp

#ip address-set s\_employee type object address 0 range 192.168.1.10 192.168.1.100

#ip service-set ftp1 type object service 0 protocol tcp source-port 10001

#policy interzone local trust inbound policy 0 action permit policy source 192.168.1.2 0

#policy interzone trust untrust outbound policy 0 action permit policy source address-set s\_employee

#policy interzone dmz untrust inbound policy 0 action permit policy service service-set ftp1 policy destination 10.1.1.2 0 policy 1 action permit policy service service-set http policy destination 10.1.1.3 0

#return