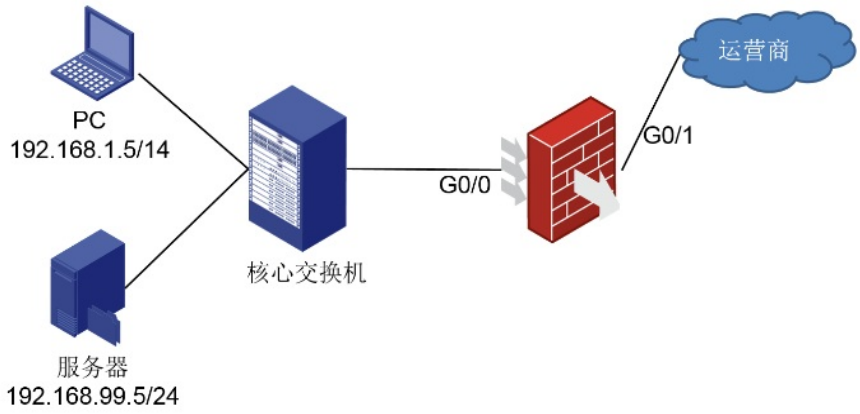
V7防火墙内网用户通过公网地址或域名访问内部服务器典型配置案例

NAT 关萌 2016-07-01 发表

1、PC和服务器的网关都在核心交换机上。
2、服务器通过nat server对外提供服务
3、PC使用DNS服务器为公网DNS。
4、PC通过域名www.aaa.com和公网IP123.1.1.1访问内网服务器。



1、定义ACL匹配内网PC地址，用于nat outbound
#B54平台版本
[F1030]acl number 3010
[F1030-acl-adv-3010]rule permit ip source 192.168.1.5 0
[F1030-acl-adv-3010]quit
#B64平台版本
[F1030-IRF]acl advanced 3010
[F1030-IRF-acl-ipv4-adv-3010]rule permit ip source 192.168.1.5 0
[F1030-IRF-acl-ipv4-adv-3010]quit
#
2、在接口G0/1上配置nat server和PC上公网的nat outbound功能。
#
[F1030]interface GigabitEthernet 0/1
[F1030-GigabitEthernet0/1nat outbound 3010
[F1030-GigabitEthernet0/1]nat server protocol tcp global 123.1.1.1 www inside 192.168.99.5 www
#
3、定义ACL匹配内网PC访问内网服务器的流量，访问服务器流量转换原地址，使服务器返回的流量经过防火墙。
#B54平台版本
[F1030]acl number 3000
[F1030-acl-adv-3000]rule permit ip source 192.168.1.5 0 destination 192.168.99.5 0
[F1030-acl-adv-3000]quit
#B64平台版本
[F1030-IRF]acl advanced 3000
[F1030-IRF-acl-ipv4-adv-3000]rule permit ip source 192.168.1.5 0 destination 192.168.99.5 0
[F1030-IRF-acl-ipv4-adv-3000]quit
#
4、在接口G0/0上配置nat server和PC访问服务器的nat outbound功能。
#
[F1030]interface GigabitEthernet 0/0
[F1030-GigabitEthernet0/2]nat outbound 3000
[F1030-GigabitEthernet0/2]nat server protocol tcp global 123.1.1.1 www inside 192.168.99.5 www
#
5、将接口G0/0和G0/1分别加入trust和untrust安全域
向安全域Trust中添加接口GigabitEthernet0/0。
system-view
[F1030] security-zone name trust
[F1030-security-zone-Trust] import interface gigabitethernet 0/0
[F1030-security-zone-Trust] quit
向安全域Untrust中添加接口GigabitEthernet0/1。

[F1030] security-zone name untrust
[F1030-security-zone-Untrust] import interface gigabitethernet 0/1
[F1030-security-zone-Untrust] quit
6、配置域间策略
配置ACL 3500，定义规则：允许IP流量。
#B54平台版本
[F1030]acl number 3500
[F1030-acl-adv-3500]rule permit ip
[F1030-acl-adv-3500]quit
#B64平台版本
[F1030] acl advanced 3500
[F1030-acl-ipv4-adv-3500] rule permit ip
[F1030-acl-ipv4-adv-3500] quit
#
创建源安全域Trust到目的安全域Untrust的安全域间实例，使Trust域用户访问Untrust域以及返回的报文可以通过。
[F1030] zone-pair security source trust destination untrust
[F1030-zone-pair-security-Trust-Untrust] packet-filter 3500
[F1030-zone-pair-security-Trust-Untrust] quit
创建源安全域Trust到目的安全域Trust的安全域间实例，使Trust域用户访问Untrust域以及返回的报文可以通过。
[F1030] zone-pair security source trust destination trust
[F1030-zone-pair-security-Trust-Untrust] packet-filter 3500
[F1030-zone-pair-security-Trust-Untrust] quit

1、在内网口配置nat server和nat outbound，nat outbound要精确匹配内网用户访问内网服务器的流量
2、配置内网安全域到内网安全的域间策略，默认情况下，同一安全域访问同一安全域的域间流量也是不放通的。