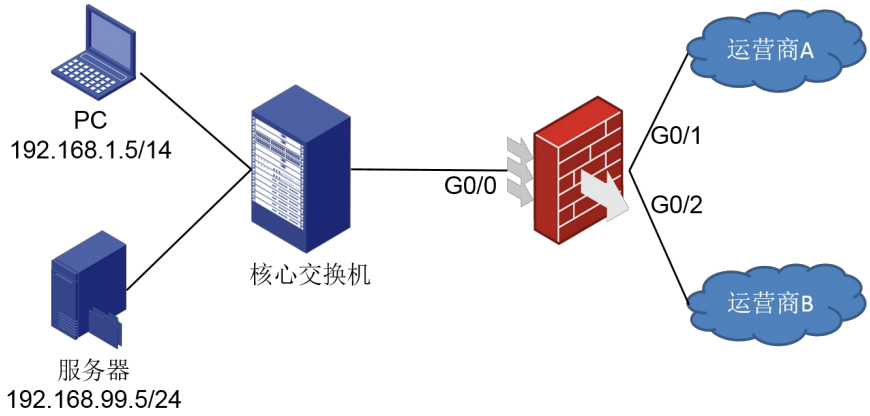
防火墙内网用户通过公网域名访问内部服务器典型配置案例集

ALG NAT 张辛 2015-07-28 发表

1、PC和服务器的网关都在核心交换机上。
2、PC通过运营商A上公网，服务器通过运营商B上公网。
3、公网用户通过运营商B访问内网服务器。
4、PC使用DNS服务器为公网DNS。
5、PC通过域名www.aaa.com访问内网服务器，公网DNS解析该域名IP为123.1.1.1。



1）防火墙开启ALG DNS功能。
核心交换机配置：
核心交换机上配置PC和服务器的网关，缺省路由指向防火墙，具体配置略。
防火墙配置：
1、在接口G0/0、G0/1、G0/2上配置相应的地址，正确配置路由和域间策略，具体配置略。
2、通过PBR将PC访问公网的流量重定向至运营商A，PC访问服务器的流量不做重定向。
#
[F1000-E-SI]acl number 3010
[F1000-E-SI-acl-adv-3010]rule permit ip source 192.168.1.5 0
[F1000-E-SI-acl-adv-3000]quit
#
[F1000-E-SI]policy-based-route PC-WAN permit node 10
[F1000-E-SI-pbr-PC-WAN-10]if-match acl 3010
[F1000-E-SI-pbr-PC-WAN-10] apply ip-address next-hop 58.1.1.2
#
[F1000-E-SI]interface GigabitEthernet 0/0
[F1000-E-SI-GigabitEthernet0/0]ip policy-based-route PC-WAN
#
3、在防火墙上开启ALG DNS功能。（缺省是关闭的，开启后配置中无显示。）
#
[F1000-E-SI]alg dns
#
4、在接口G0/1上配置nat server和PC上公网的nat outbound功能。
#
[F1000-E-SI]interface GigabitEthernet 0/1
[F1000-E-SI-GigabitEthernet0/1nat outbound 3010
[F1000-E-SI-GigabitEthernet0/1]nat server protocol tcp global 123.1.1.1 www inside 192.168.99.5 ww
w
#
5、在接口G0/2上配置nat server和服务器上公网的nat outbound功能。
[F1000-E-SI]acl number 3020
[F1000-E-SI-acl-adv-3020]rule permit ip source 192.168.99.5 0
[F1000-E-SI-acl-adv-3020]quit
#
[F1000-E-SI]interface GigabitEthernet 0/2
[F1000-E-SI-GigabitEthernet0/2]nat outbound 3020
[F1000-E-SI-GigabitEthernet0/2]nat server protocol tcp global 123.1.1.1 www inside 192.168.99.5 ww
w

#
完整配置：
#
 undo alg ftp
 undo alg rtsp
 undo alg h323
 undo alg sip
 undo alg sqlnet
 undo alg pptp
 undo alg ils
 undo alg nbt
 undo alg msn
 undo alg qq
 undo alg tftp
 undo alg sccp
 undo alg gtp
#
acl number 3010
 rule 0 permit ip source 192.168.1.5 0
acl number 3020
 rule 0 permit ip source 192.168.99.5 0
#
policy-based-route PC-WAN permit node 10
 if-match acl 3010
 apply ip-address next-hop 58.1.1.2
#
interface GigabitEthernet0/0
 port link-mode route
 ip address 192.168.255.1 255.255.255.252
 ip policy-based-route PC-WAN
#
interface GigabitEthernet0/1
 port link-mode route
 nat outbound 3010
 nat server protocol tcp global 123.1.1.1 www inside 192.168.99.5 www
 ip address 58.1.1.1 255.255.255.252
#
interface GigabitEthernet0/2
 port link-mode route
 nat outbound 3020
 nat server protocol tcp global 123.1.1.1 www inside 192.168.99.5 www
 ip address 202.2.2.1 255.255.255.252
#
 ip route-static 0.0.0.0 0.0.0.0 202.2.2.2
 ip route-static 192.168.0.0 255.255.0.0 192.168.255.2
#

2）防火墙不开启ALG DNS功能。
核心交换机配置：
核心交换机上配置PC和服务器的网关，缺省路由指向防火墙，具体配置略。
防火墙配置：
1、在接口G0/0、G0/1、G0/2上配置相应的地址，正确配置路由和域间策略，具体配置略。
2、通过PBR将PC访问公网的流量重定向至运营商A，PC访问服务器的流量不做重定向。
#
[F1000-E-SI]acl number 3000
[F1000-E-SI-acl-adv-3000]rule permit ip source 192.168.1.5 0 destination 192.168.99.5 0
[F1000-E-SI-acl-adv-3000]quit
#
[F1000-E-SI]acl number 3010
[F1000-E-SI-acl-adv-3010]rule permit ip source 192.168.1.5 0
[F1000-E-SI-acl-adv-3000]quit
#
[F1000-E-SI]policy-based-route PC-WAN deny node 5
[F1000-E-SI-pbr-PC-WAN-5]if-match acl 3000

[F1000-E-SI-pbr-PC-WAN-5]quit
[F1000-E-SI]policy-based-route PC-WAN permit node 10
[F1000-E-SI-pbr-PC-WAN-10]if-match acl 3010
[F1000-E-SI-pbr-PC-WAN-10] apply ip-address next-hop 58.1.1.2
#
[F1000-E-SI]interface GigabitEthernet 0/0
[F1000-E-SI-GigabitEthernet0/0]ip policy-based-route PC-WAN
#
3、在接口G0/0上配置nat server和PC访问服务器的nat outbound功能。
#
[F1000-E-SI]interface GigabitEthernet 0/0
[F1000-E-SI-GigabitEthernet0/2]nat outbound 3000
[F1000-E-SI-GigabitEthernet0/2]nat server protocol tcp global 123.1.1.1 www inside 192.168.99.5 ww
w
#
4、在接口G0/1上配置PC上公网的nat outbound功能。
#
[F1000-E-SI]interface GigabitEthernet 0/1
[F1000-E-SI-GigabitEthernet0/2]nat outbound 3010
#
5、在接口G0/2上配置nat server和服务器上公网的nat outbound功能。
[F1000-E-SI]acl number 3020
[F1000-E-SI-acl-adv-3020]rule permit ip source 192.168.99.5 0
[F1000-E-SI-acl-adv-3020]quit
#
[F1000-E-SI]interface GigabitEthernet 0/2
[F1000-E-SI-GigabitEthernet0/2]nat outbound 3020
[F1000-E-SI-GigabitEthernet0/2]nat server protocol tcp global 123.1.1.1 www inside 192.168.99.5 ww
w
#
完整配置:
#
 undo alg all
#
acl number 3000
 rule 5 permit ip source 192.168.1.5 0 destination 192.168.99.5 0
acl number 3010
 rule 0 permit ip source 192.168.1.5 0
acl number 3020
 rule 0 permit ip source 192.168.99.5 0
#
policy-based-route PC-WAN deny node 5
 if-match acl 3000
policy-based-route PC-WAN permit node 10
 if-match acl 3010
 apply ip-address next-hop 58.1.1.2
#
interface GigabitEthernet0/0
 port link-mode route
nat outbound 3000
 nat server protocol tcp global 123.1.1.1 www inside 192.168.99.5 www
 ip address 192.168.255.1 255.255.255.252
 ip policy-based-route PC-WAN
#
interface GigabitEthernet0/1
 port link-mode route
 nat outbound 3010
ip address 58.1.1.1 255.255.255.252
#
interface GigabitEthernet0/2
 port link-mode route
 nat outbound 3020
 nat server protocol tcp global 123.1.1.1 www inside 192.168.99.5 www
 ip address 202.2.2.1 255.255.255.252

#
 ip route-static 0.0.0.0 0.0.0.0 202.2.2.2
 ip route-static 192.168.0.0 255.255.0.0 192.168.255.2
#

1、在接口同时配置有PBR和NAT的情况下，报文优先匹配NAT。做完NAT转换后，再进行PBR匹配。
2、开启ALG DNS功能时，PC通过域名访问服务器时，只需要在防火墙公网DNS报文入接口上配置相应的NAT SERVER，设备会自动将DNS报文中的公网地址替换为NAT SERVER映射的内网地址。防火墙内网口不需要做任何配置。
3、不开启ALG DNS功能时，PC通过域名访问服务器时，要在防火墙内网口配置NAT SERVER和NAT OUTBOUND，使PC访问服务器的流量通过防火墙绕行，保障来回路径一致。同时保证PC访问服务器的流量不被PBR做重定向。
4、如果客户要使用公网地址访问内网服务器，则需使用方案二。