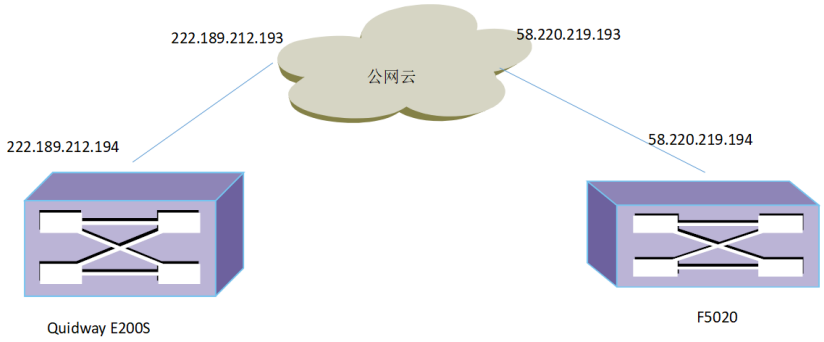
某地址，通过手机流量可以正常访问，通过F5020就不可以访问

域间策略/安全域 Web页面 zhiliao_2STJa 2017-11-21 发表

组网及说明

华为防火墙地址：222.189.212.194 默认路由到222.189.212.193



F5020：地址58.220.219.194 默认路由到58.220.219.193
华为上面做了端口映射，吧服务器的映射到公网。目前通过手机流量和酒店网络都可以正常访问http://222.189.212.198:8081/eGovaMIS/login.htm
但是在F5020下面的终端，可以正常上网，却不能访问华为防火墙映射出的地址。改地址不可ping，但可以个telnet登录

具体配置如下。望大神可以解决

F5020：

```
[chukou-FW]dis cu
#
 version 7.1.064, Release 9310P12
#
 sysname chukou-FW
#
context Admin id 1
#
ip vpn-instance management
 route-distinguisher 1000000000:1
 vpn-target 1000000000:1 import-extcommunity
 vpn-target 1000000000:1 export-extcommunity
#
 telnet server enable
#
 irf mac-address persistent timer
 irf auto-update enable
 undo irf link-delay
 irf member 1 priority 10
 irf member 2 priority 1
#
 ip pool l2tp 10.155.222.1 10.155.223.254
#
nat address-group 1
 address 58.220.219.194 58.220.219.194
#
 password-recovery enable
#
vlan 1
#
vlan 10
#
vlan 4001
```

```
#
irf-port 1/1
 port group interface Ten-GigabitEthernet1/0/26
 port group interface Ten-GigabitEthernet1/0/27
#
irf-port 2/2
 port group interface Ten-GigabitEthernet2/0/26
 port group interface Ten-GigabitEthernet2/0/27
#
object-group ip address myip
 0 network host address 10.155.245.136
 10 network host address 58.220.219.194
#
object-group service mysvr
 0 service tcp destination eq 3389
 10 service tcp destination eq 5901
 20 service tcp destination eq 22
 30 service tcp destination eq 8080
 40 service tcp destination eq 8443
 50 service udp destination eq 1701
 60 service tcp destination eq 5900
#
interface Reth1
 description to_zhenwuwaiwang_s105
 ip address 10.155.253.254 255.255.255.252
 member interface Ten-GigabitEthernet1/0/24 priority 255
 member interface Ten-GigabitEthernet2/0/24 priority 50
 packet-filter 2500 inbound
#
interface Reth2
 description TO_S9810_hulian
 ip address 10.155.241.254 255.255.255.252
 member interface Ten-GigabitEthernet1/0/25 priority 255
 member interface Ten-GigabitEthernet2/0/25 priority 50
#
interface Bridge-Aggregation1
 port access vlan 10
 link-aggregation mode dynamic
#
interface Bridge-Aggregation2
 description waiwangjinxian
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4001
#
interface Virtual-Template1
 ppp authentication-mode chap
 remote address pool l2tp
 ip address 10.155.223.254 255.255.254.0
#
interface NULL0
#
interface Vlan-interface10
#
interface Vlan-interface4001
 ip address 58.220.219.194 255.255.255.192
 nat outbound 2000 address-group 1
 nat server protocol tcp global 58.220.219.200 122 inside 10.155.245.132 22
 nat server protocol tcp global 58.220.219.200 5901 inside 10.155.245.1 5901
 nat server protocol tcp global 58.220.219.201 8443 inside 10.155.245.200 3389
 nat server protocol tcp global current-interface 4422 inside 10.155.253.253 22
 nat server protocol tcp global current-interface 5002 inside 10.155.245.1 8443
 nat server protocol tcp global current-interface 5003 inside 10.155.245.129 3389
 ipsec apply policy 1
```

```
#
interface GigabitEthernet1/0/0
 port link-mode route
 ip binding vpn-instance management
 ip address 192.168.0.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode route
#
interface GigabitEthernet1/0/3
 port link-mode route
 ip address 10.155.242.1 255.255.255.128
#
interface GigabitEthernet1/0/4
 port link-mode route
#
interface GigabitEthernet1/0/5
 port link-mode route
#
interface GigabitEthernet1/0/6
 port link-mode route
#
interface GigabitEthernet1/0/7
 port link-mode route
#
interface GigabitEthernet1/0/8
 port link-mode route
#
interface GigabitEthernet1/0/9
 port link-mode route
#
interface GigabitEthernet1/0/10
 port link-mode route
#
interface GigabitEthernet1/0/11
 port link-mode route
#
interface GigabitEthernet1/0/16
 port link-mode route
#
interface GigabitEthernet1/0/17
 port link-mode route
#
interface GigabitEthernet1/0/18
 port link-mode route
#
interface GigabitEthernet1/0/19
 port link-mode route
#
interface GigabitEthernet1/0/20
 port link-mode route
#
interface GigabitEthernet1/0/21
 port link-mode route
#
interface GigabitEthernet1/0/22
 port link-mode route
#
interface GigabitEthernet1/0/23
 port link-mode route
#
interface GigabitEthernet2/0/0
 port link-mode route
#
```

```
interface GigabitEthernet2/0/1
 port link-mode route
#
interface GigabitEthernet2/0/2
 port link-mode route
#
interface GigabitEthernet2/0/3
 port link-mode route
#
interface GigabitEthernet2/0/4
 port link-mode route
#
interface GigabitEthernet2/0/5
 port link-mode route
#
interface GigabitEthernet2/0/6
 port link-mode route
#
interface GigabitEthernet2/0/7
 port link-mode route
#
interface GigabitEthernet2/0/8
 port link-mode route
#
interface GigabitEthernet2/0/9
 port link-mode route
#
interface GigabitEthernet2/0/10
 port link-mode route
#
interface GigabitEthernet2/0/11
 port link-mode route
#
interface GigabitEthernet2/0/12
 port link-mode route
#
interface GigabitEthernet2/0/13
 port link-mode route
#
interface GigabitEthernet2/0/14
 port link-mode route
#
interface GigabitEthernet2/0/15
 port link-mode route
#
interface GigabitEthernet2/0/16
 port link-mode route
#
interface GigabitEthernet2/0/17
 port link-mode route
#
interface GigabitEthernet2/0/18
 port link-mode route
#
interface GigabitEthernet2/0/19
 port link-mode route
#
interface GigabitEthernet2/0/20
 port link-mode route
#
interface GigabitEthernet2/0/21
 port link-mode route
#
interface GigabitEthernet2/0/22
```

```
 port link-mode route
#
interface GigabitEthernet2/0/23
 port link-mode route
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-aggregation group 1
#
interface GigabitEthernet1/0/12
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4001
 speed 1000
 duplex full
 port link-aggregation group 2
#
interface GigabitEthernet1/0/13
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4001
 speed 1000
 duplex full
 port link-aggregation group 2
#
interface GigabitEthernet1/0/14
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4001
 speed 1000
 duplex full
 port link-aggregation group 2
#
interface GigabitEthernet1/0/15
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
#
interface Ten-GigabitEthernet1/0/24
 port link-mode route
 packet-filter 3000 inbound
#
interface Ten-GigabitEthernet1/0/25
 port link-mode route
#
interface Ten-GigabitEthernet2/0/24
 port link-mode route
#
interface Ten-GigabitEthernet2/0/25
 port link-mode route
#
interface Ten-GigabitEthernet1/0/26
#
interface Ten-GigabitEthernet1/0/27
#
interface Ten-GigabitEthernet2/0/26
#
interface Ten-GigabitEthernet2/0/27
#
object-policy ip Local-Untrust
 rule 0 pass source-ip myip counting
```

```
#
object-policy ip all.pass
 rule 0 pass counting
#
object-policy ip mypolicy
 rule 0 pass service mysvr counting
 rule 1 pass destination-ip myip counting
#
security-zone name Local
#
security-zone name Trust
 import interface GigabitEthernet1/0/3
 import interface Reth1
 import interface Virtual-Template1
#
security-zone name DMZ
 import interface Reth2
#
security-zone name Untrust
 import interface Vlan-interface4001
 import interface Bridge-Aggregation2 vlan 4001
 import interface GigabitEthernet1/0/12 vlan 4001
 import interface GigabitEthernet1/0/13 vlan 4001
 import interface GigabitEthernet1/0/14 vlan 4001
#
security-zone name Management
 import interface GigabitEthernet1/0/0
#
zone-pair security source Any destination Any
 object-policy apply ip all.pass
#
zone-pair security source DMZ destination Trust
 object-policy apply ip all.pass
#
zone-pair security source Local destination Trust
 object-policy apply ip all.pass
#
zone-pair security source Local destination Untrust
 object-policy apply ip Local-Untrust
#
zone-pair security source Trust destination Trust
 object-policy apply ip all.pass
#
zone-pair security source Untrust destination Local
 object-policy apply ip mypolicy
#
zone-pair security source Untrust destination Trust
 object-policy apply ip mypolicy
#
 scheduler logfile size 16
#
line class console
 user-role network-admin
#
line class vty
 user-role network-operator
#
line con 0 1
 authentication-mode scheme
 user-role network-admin
#
line vty 0 4
 authentication-mode scheme
 user-role level-15
```

```
 user-role network-admin
 protocol inbound telnet
#
line vty 5 63
 authentication-mode scheme
 user-role network-admin
#
 ip route-static 0.0.0.0 0 58.220.219.193
 ip route-static 10.155.0.0 16 10.155.253.253
 ip route-static 10.155.241.0 24 10.155.241.253
 ip route-static 10.155.242.0 23 10.155.241.253
 ip route-static 10.155.244.0 24 10.155.241.253
 ip route-static 32.0.0.0 8 10.155.253.253
 ip route-static 59.192.0.0 10 10.155.253.253
 ip route-static 100.64.0.0 10 10.155.253.253
 ip route-static 172.21.0.0 17 10.155.253.253
 ip route-static 172.23.0.0 16 10.155.253.253
 ip route-static 172.24.0.0 16 10.155.253.253
 ip route-static 222.189.0.0 16 58.220.219.193
#
 info-center loghost 10.155.245.129
#
 snmp-agent
 snmp-agent local-engineid 800063A2809C061BFC3E9200000001
 snmp-agent community write Admin@2017.yz
 snmp-agent community read Admin@2017.yzzww
 snmp-agent community read yizheng
 snmp-agent community write yzzww
 snmp-agent sys-info version all
 snmp-agent target-host trap address udp-domain 10.155.245.129 params securityname Admin@201
7.yz
 snmp-agent target-host trap address udp-domain 10.155.245.129 params securityname jscegn@yc
 snmp-agent target-host trap address udp-domain 10.155.245.129 params securityname yizheng v2c
 snmp-agent trap enable arp
 snmp-agent trap enable radius
 snmp-agent trap enable syslog
 snmp-agent trap queue-size 500
 snmp-agent trap life 600
#
 ssh server enable
#
redundancy group aaa
 member interface Reth1
 member interface Reth2
 node 1
  bind slot 1
  priority 100
  track 1 interface Ten-GigabitEthernet1/0/24
  track 3 interface Ten-GigabitEthernet1/0/25
 node 2
  bind slot 2
  priority 50
  track 2 interface Ten-GigabitEthernet2/0/24
  track 4 interface Ten-GigabitEthernet2/0/25
#
acl basic 2000
 rule 0 permit source 10.155.2.0 0.0.0.255
 rule 5 permit source 10.155.222.0 0.0.1.255
 rule 10 permit
#
acl basic 2500
 rule 0 permit source 10.155.222.0 0.0.1.255
#
 radius session-control enable
```

```
#
radius scheme l2tp
 primary authentication 10.155.245.129
 primary accounting 10.155.245.129
 key authentication cipher $c$3$Ch8qoRL/xO4+0HkmONp0OkJDdJ8BY2mj
 key accounting cipher $c$3$/a5gXRupGQYi8CwNyGhrHooHQIjo7T6B
 user-name-format without-domain
 nas-ip 10.155.253.254
#
domain l2tp
 authentication portal radius-scheme l2tp
 authorization portal radius-scheme l2tp
 accounting portal radius-scheme l2tp
#
domain system
 authentication ppp radius-scheme l2tp
 authorization ppp radius-scheme l2tp
 accounting ppp radius-scheme l2tp
#
 aaa session-limit ftp 16
 aaa session-limit telnet 16
 aaa session-limit ssh 16
 domain default enable system
#
role name level-0
 description Predefined level-0 role
#
role name level-1
 description Predefined level-1 role
#
role name level-2
 description Predefined level-2 role
#
role name level-3
 description Predefined level-3 role
#
role name level-4
 description Predefined level-4 role
#
role name level-5
 description Predefined level-5 role
#
role name level-6
 description Predefined level-6 role
#
role name level-7
 description Predefined level-7 role
#
role name level-8
 description Predefined level-8 role
#
role name level-9
 description Predefined level-9 role
#
role name level-10
 description Predefined level-10 role
#
role name level-11
 description Predefined level-11 role
#
role name level-12
 description Predefined level-12 role
#
role name level-13
```

```
 description Predefined level-13 role
#
role name level-14
 description Predefined level-14 role
#
user-group system
#
local-user admin class manage
 password hash
$h$6$pKuRW2tehlA/EIWa$l/fHQ9bdhTNBEih59RC5pOVGwc06UqEyFxWguMDSzp6bgjTwSj+fgtqJzF
wVwMVUkjYtGlNx3slJmNtCKnmlXw==
 service-type ssh telnet terminal https
 authorization-attribute user-role level-3
 authorization-attribute user-role level-15
 authorization-attribute user-role network-admin
 authorization-attribute user-role network-operator
#
local-user h3c class manage
 password hash
$h$6$jLOMRMQpGDbBPmjq$Ub4NR+5jh3kVoMB07c5XdnqXdyOnKRTAb16XXEe7KMPgWrDWdCo
vlputGEB6oL3k9yhhnLL+27mpxYMtMAOnyA==
 service-type telnet https
 authorization-attribute user-role level-15
 authorization-attribute user-role network-admin
 authorization-attribute user-role network-operator
#
local-user zp class manage
 password hash $h$6$ppXWGvgDjlbDxTWu$0Bdbzx+hNYvTGGy9jZB7pg/KFlfIraHrJdXjZfEdR9rHXc
A3/8/+SJe5h8tK+QOBwOm5/i6pxDOa53LBsYfIlw==
 service-type telnet http https
 authorization-attribute user-role level-15
 authorization-attribute user-role network-operator
#
local-user ?   class manage
 authorization-attribute user-role network-operator
#
local-user admi class network
 authorization-attribute user-role network-operator
#
local-user admin class network
 password cipher $c$3$Hq7PSbHzKtZjhFVCy7T2KXPGRXw0IVbR
 service-type ppp
 authorization-attribute user-role network-operator
#
local-user tk class network
 password cipher $c$3$bkAuol9t9z5Plc87jJqRp7X42SxcaGhepOo9
 service-type ppp
 authorization-attribute user-role network-operator
#
ssl server-policy king
#
 session statistics enable
 session synchronization enable
#
ipsec transform-set l2tp
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm sha1
#
ipsec policy-template l2tp 10
 transform-set l2tp
 ike-profile l2tp
#
ipsec policy 1 10 isakmp template l2tp
#
```

```
l2tp-group 1 mode lns
 allow l2tp virtual-template 1 remote LAC
 undo tunnel authentication
 tunnel name LNS
#
 l2tp enable
#
 ike identity fqdn lns
#
ike profile l2tp
 keychain l2tp
 exchange-mode aggressive
 local-identity fqdn lns
 match remote identity fqdn l2tp
 proposal 1
#
ike proposal 1
 encryption-algorithm 3des-cbc
#
ike keychain l2tp
 pre-shared-key hostname l2tp key cipher $c$3$HpDpx95Gi8AcwZDS+8+JKcmgi3GGKCfX2kWc
#
 ip http enable
 ip https enable
#
inspect block-source parameter-profile ips_block_default_parameter
#
inspect capture parameter-profile ips_capture_default_parameter
#
inspect logging parameter-profile ips_logging_default_parameter
#
inspect redirect parameter-profile av_redirect_default_parameter
#
inspect redirect parameter-profile ips_redirect_default_parameter
#
inspect redirect parameter-profile url_redirect_default_parameter
#
ips policy default
#
anti-virus policy default
#
 track 1 interface Ten-GigabitEthernet1/0/24 physical
 track 2 interface Ten-GigabitEthernet2/0/24 physical
 track 3 interface Ten-GigabitEthernet1/0/25 physical
 track 4 interface Ten-GigabitEthernet2/0/25 physical
#
return
```

Quidway E200S

```
<Eudemon> dis cu
#
 sysname Eudemon
#
 super password level 3 simple 123456
#
  web-manager enable
#
 l2tp enable
#
 firewall packet-filter default permit interzone trust untrust direction inbound
 firewall packet-filter default permit interzone trust untrust direction outbound
#
 nat address-group 1 222.189.212.195 222.189.212.207
 nat server protocol tcp global 222.189.212.195 3389 inside 192.168.2.100 3389
```

```
 nat server protocol tcp global 222.189.212.200 www inside 192.168.2.101 www
 nat server protocol tcp global 222.189.212.200 3389 inside 192.168.2.101 3389
 nat server protocol tcp global 222.189.212.201 3389 inside 192.168.2.102 3389
 nat server protocol tcp global 222.189.212.202 3389 inside 172.16.88.102 3389
 nat server protocol tcp global 222.189.212.195 www inside 192.168.2.100 www
 nat server protocol tcp global 222.189.212.195 7080 inside 192.168.2.100 7080
 nat server protocol tcp global 222.189.212.195 8600 inside 192.168.2.100 8600
 nat server protocol tcp global 222.189.212.200 2000 inside 192.168.2.101 2000
 nat server  global 222.189.212.196 inside 192.168.2.50
 nat server protocol tcp global 222.189.212.195 2000 inside 192.168.2.100 2000
 nat server protocol tcp global 222.189.212.197 3389 inside 192.168.2.105 3389
 nat server protocol tcp global 222.189.212.197 www inside 192.168.2.105 www
 nat server protocol tcp global 222.189.212.201 www inside 192.168.2.102 www
 nat server protocol tcp global 222.189.212.198 3389 inside 192.168.2.20 3389
 nat server protocol tcp global 222.189.212.198 www inside 192.168.2.20 www
 nat server protocol tcp global 222.189.212.199 www inside 192.168.2.21 www
 nat server protocol tcp global 222.189.212.199 3389 inside 192.168.2.21 3389
 nat server protocol tcp global 222.189.212.198 8081 inside 192.168.2.20 8081
 nat server protocol tcp global 222.189.212.198 8082 inside 192.168.2.20 8082
 nat server protocol tcp global 222.189.212.198 8083 inside 192.168.2.20 8083
 nat server protocol tcp global 222.189.212.198 8084 inside 192.168.2.20 8084
 nat server protocol tcp global 222.189.212.198 8085 inside 192.168.2.20 8085
 nat server protocol tcp global 222.189.212.198 8181 inside 192.168.2.20 8181
 nat server protocol tcp global 222.189.212.198 telnet inside 192.168.2.20 telnet
 nat server protocol tcp global 222.189.212.199 8399 inside 192.168.2.21 8399
 nat server protocol tcp global 222.189.212.199 8081 inside 192.168.2.21 8081
 nat server protocol tcp global 222.189.212.199 8082 inside 192.168.2.21 8082
 nat server protocol tcp global 222.189.212.199 8083 inside 192.168.2.21 8083
 nat server protocol tcp global 222.189.212.199 8084 inside 192.168.2.21 8084
 nat server protocol tcp global 222.189.212.199 8085 inside 192.168.2.21 8085
 nat server protocol tcp global 222.189.212.199 8181 inside 192.168.2.21 8181
 nat alg enable ftp
 nat alg enable dns
 nat alg enable icmp
 nat alg enable netbios
 undo nat alg enable h323
 undo nat alg enable hwcc
 undo nat alg enable ils
 undo nat alg enable pptp
 undo nat alg enable qq
 undo nat alg enable msn
 undo nat alg enable user-define
 undo nat alg enable sip
 undo nat alg enable rtsp
 firewall permit sub-ip
#
 firewall blacklist enable
 firewall blacklist item 187.58.63.5
 firewall blacklist item 59.175.193.82
#
 firewall defend ip-spoofing enable
 firewall defend land enable
 firewall defend smurf enable
 firewall defend fraggle enable
 firewall defend winnuke enable
 firewall defend syn-flood enable
 firewall defend udp-flood enable
 firewall defend icmp-flood enable
 firewall defend icmp-redirect enable
 firewall defend icmp-unreachable enable
 firewall defend ip-sweep enable
 firewall defend port-scan enable
 firewall defend source-route enable
 firewall defend route-record enable
```

```
 firewall defend tracert enable
 firewall defend time-stamp enable
 firewall defend ping-of-death enable
 firewall defend teardrop enable
 firewall defend tcp-flag enable
 firewall defend ip-fragment enable
 firewall defend large-icmp enable
#
 firewall statistic system enable
#
interface Aux0
 async mode flow
 link-protocol ppp
#
interface Ethernet0/0/0
 ip address 222.189.212.194 255.255.255.240
#
interface Ethernet0/0/1
 ip address 192.168.2.1 255.255.255.0
 ip address 172.16.88.1 255.255.255.0 sub
#
interface Ethernet0/0/2
#
interface Ethernet0/0/3
#
interface Ethernet0/0/4
#
interface Virtual-Template1
 ppp authentication-mode chap
 ip address 172.16.87.1 255.255.255.0
 remote address pool 1
#
interface Tunnel1
#
interface Secp0/0/0
#
interface NULL0
#
acl number 2012
 rule 0 permit source 192.168.0.0 0.0.255.255
 rule 1 permit source 172.16.88.0 0.0.0.255
acl number 2101
 rule 0 permit source 192.168.2.0 0.0.0.255
 rule 1 permit source 172.16.88.0 0.0.0.255
#
acl number 3101
 rule 1 permit tcp source 192.168.2.0 0.0.0.255 destination 202.102.112.14 0
 rule 2 permit tcp source 172.16.88.0 0.0.0.255 destination 202.102.112.14 0
 rule 5 permit ip source 192.168.2.101 0
acl number 3102
 rule 0 permit tcp source 218.91.0.0 0.0.255.255 destination 192.168.2.0 0.0.0.255 destination-port e
q www
 rule 1 permit tcp source 221.229.0.0 0.0.255.255 destination 192.168.2.0 0.0.0.255 destination-port
eq www
 rule 2 permit tcp source 61.177.184.0 0.0.0.255 destination 192.168.2.0 0.0.0.255 destination-port e
q www
 rule 3 permit tcp source 58.220.0.0 0.0.255.255 destination 192.168.2.0 0.0.0.255 destination-port e
q www
 rule 4 permit tcp source 117.61.84.0 0.0.0.255 destination 192.168.2.0 0.0.0.255 destination-port eq
www
 rule 5 permit tcp source 117.61.87.0 0.0.0.255 destination 192.168.2.0 0.0.0.255 destination-port eq
www
 rule 6 permit tcp source 222.189.0.0 0.0.255.255 destination 192.168.2.0 0.0.0.255 destination-port
eq www
```

rule 7 permit tcp source 121.233.0.0 0.0.255.255 destination 192.168.2.0 0.0.0.255 destination-port eq www
rule 8 permit tcp destination 192.168.2.100 0 destination-port eq 7080
rule 9 permit tcp destination 192.168.2.100 0 destination-port eq 8600
rule 10 permit tcp source 218.91.0.0 0.0.255.255 destination 172.16.88.0 0.0.0.255 destination-port eq www
rule 11 permit tcp source 221.229.0.0 0.0.255.255 destination 172.16.88.0 0.0.0.255 destination-port eq www
rule 12 permit tcp source 61.177.184.0 0.0.0.255 destination 172.16.88.0 0.0.0.255 destination-port eq www
rule 13 permit tcp source 58.220.0.0 0.0.255.255 destination 172.16.88.0 0.0.0.255 destination-port eq www
rule 14 permit tcp source 117.61.84.0 0.0.0.255 destination 172.16.88.0 0.0.0.255 destination-port eq www
rule 15 permit tcp source 117.61.87.0 0.0.0.255 destination 172.16.88.0 0.0.0.255 destination-port eq www
rule 16 permit tcp source 222.189.0.0 0.0.255.255 destination 172.16.88.0 0.0.0.255 destination-port eq www
rule 17 permit tcp source 121.233.0.0 0.0.255.255 destination 172.16.88.0 0.0.0.255 destination-port eq www
rule 18 permit tcp source 180.0.0.0 0.255.255.255 destination 192.168.2.0 0.0.0.255 destination-port eq www
rule 19 permit tcp source 180.0.0.0 0.255.255.255 destination 172.16.88.0 0.0.0.255 destination-port eq www
rule 20 permit tcp source 211.103.30.165 0 destination 192.168.2.0 0.0.0.255 destination-port eq www
rule 22 permit tcp destination 192.168.2.0 0.0.0.255 destination-port eq 3389
rule 24 permit tcp source 122.195.136.168 0 destination 192.168.2.0 0.0.0.255 destination-port eq www
rule 25 permit tcp source 121.229.89.213 0 destination 192.168.2.0 0.0.0.255 destination-port eq www
rule 26 permit tcp source 221.6.166.2 0 destination 192.168.2.0 0.0.0.255 destination-port eq www
rule 27 permit tcp source 198.17.120.227 0 destination 192.168.2.0 0.0.0.255 destination-port eq www
rule 29 permit tcp source 61.177.181.138 0 destination 192.168.2.0 0.0.0.255 destination-port eq www
rule 30 permit tcp source 221.130.68.99 0 destination 192.168.2.0 0.0.0.255 destination-port eq www
rule 31 permit tcp source 61.177.181.2 0 destination 192.168.2.0 0.0.0.255 destination-port eq www
rule 32 permit tcp source 58.220.231.2 0 destination 192.168.2.0 0.0.0.255 destination-port eq www
rule 33 permit tcp source 121.229.89.0 0.0.0.255 destination 192.168.2.0 0.0.0.255 destination-port eq www
rule 34 permit tcp source 202.102.23.0 0.0.0.255 destination 192.168.2.0 0.0.0.255 destination-port eq www
rule 35 permit tcp source 211.103.38.0 0.0.0.255 destination 192.168.2.0 0.0.0.255 destination-port eq www
rule 36 permit tcp source 114.230.0.0 0.0.255.255 destination 192.168.2.0 0.0.0.255 destination-port eq www
rule 39 permit tcp source 117.91.0.0 0.0.255.255 destination 192.168.2.0 0.0.0.255 destination-port eq www
rule 40 permit tcp source 58.241.129.90 0 destination 192.168.2.0 0.0.0.255 destination-port eq www
rule 41 permit tcp source 211.103.35.35 0 destination 192.168.2.0 0.0.0.255 destination-port eq www
rule 42 permit tcp source 61.132.36.18 0 destination 192.168.2.50 0 destination-port eq 3306
rule 43 permit tcp source 61.147.75.148 0 destination 192.168.2.50 0 destination-port eq 3306
rule 45 permit tcp source 122.194.0.0 0.0.255.255 destination 192.168.0.0 0.0.0.255 destination-port eq www
rule 46 permit tcp source 58.220.0.0 0.0.255.255 destination 192.168.0.0 0.0.0.255 destination-port eq www
rule 50 permit tcp source 58.220.0.0 0.0.255.255 destination 192.168.2.0 0.0.0.255
rule 52 permit tcp source 58.220.0.0 0.0.255.255 destination 192.168.0.0 0.0.255.255 destination-port eq www
rule 54 permit ip source 58.220.0.0 0.0.255.255 destination 192.168.2.0 0.0.0.255

```
 rule 56 permit tcp source 58.220.0.0 0.0.255.255 destination 192.168.2.0 0.0.0.255 destination-port
eq telnet

 rule 100 permit ip source 202.102.112.14 0 destination 192.168.2.0 0.0.0.255
 rule 101 permit ip source 202.102.112.14 0 destination 172.16.88.0 0.0.0.255
 rule 102 permit ip source 61.147.75.143 0 destination 192.168.2.0 0.0.0.255
 rule 200 permit ip destination 192.168.2.0 0.0.0.255
acl number 3103
 rule 0 permit tcp source 202.102.112.14 0 destination 222.189.212.194 0
 rule 1 permit udp destination 222.189.212.194 0 destination-port eq 1701
 rule 3 permit tcp destination 222.189.212.194 0

acl number 3104
 rule 0 permit tcp source 172.16.87.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
 rule 1 permit tcp source 172.16.87.0 0.0.0.255 destination 172.16.88.0 0.0.0.255
#
firewall zone local
 set priority 100
#
firewall zone trust
 set priority 85
 add interface Ethernet0/0/1
#
firewall zone untrust
 set priority 5
 add interface Ethernet0/0/0
#
firewall zone dmz
 set priority 50
#
firewall zone name vpnzone
 set priority 60
 add interface Virtual-Template1
#
firewall interzone local trust
#
firewall interzone local untrust
 packet-filter 3103 inbound
#
firewall interzone local dmz
#
firewall interzone local vpnzone
#
firewall interzone trust untrust
 nat outbound 2101 address-group 1
 detect ftp
 detect http
#
firewall interzone trust dmz
#
firewall interzone trust vpnzone
 packet-filter 3104 inbound
#
firewall interzone dmz untrust
#
firewall interzone vpnzone untrust
#
firewall interzone vpnzone dmz
#
l2tp-group 1
 undo tunnel authentication
 allow l2tp virtual-template 1
#
aaa
```

```
 local-user vpn03 password simple jshxszcgvpn03
 local-user vpn03 service-type ppp
 local-user vpn04 password simple jshxszcgvpn04
 local-user vpn04 service-type ppp
 local-user awingsky password simple song-3332chaoqin
 local-user awingsky service-type web
 local-user awingsky level 3
 local-user callcenter01 password simple callcenter01
 local-user callcenter01 service-type ppp
 local-user callcenter02 password simple callcenter01
 local-user callcenter02 service-type ppp
 local-user vpn05 password simple jshxszcgvpn05
 local-user vpn05 service-type ppp
 local-user admin password simple song-3332chaoqin
 local-user admin service-type web telnet
 local-user admin level 1
 local-user vpn01 password simple jshxszcgvpn01
 local-user vpn01 service-type ppp
 local-user songchaoqin password simple song-3332chaoqin
 local-user songchaoqin service-type web telnet ssh
 local-user vpn06 password simple jshxszcgvpn06
 local-user vpn06 service-type ppp
 local-user vpn02 password simple jshxszcgvpn02
 local-user vpn02 service-type ppp
 local-user vpn07 password simple jshxszcgvpn07
 local-user vpn07 service-type ppp
 ip pool 1 172.16.87.50 172.16.87.254
#
 authentication-scheme default
 authentication-scheme login
#
 authorization-scheme default
#
 accounting-scheme default
#
 domain default
#
#
 ip route-static 0.0.0.0 0.0.0.0 222.189.212.193
 ip route-static 58.220.0.0 255.255.0.0 222.189.212.193
 ip route-static 58.220.0.0 255.255.0.0 58.220.219.193
#
user-interface con 0
user-interface aux 0
user-interface vty 0 4
 authentication-mode aaa
 user privilege level 1
#
return
```

问题描述

现有华为防火墙E200S。下挂服务器，做端口映射。在公网上面可以访问映射出去的地址。
http://222.189.212.198:8081/eGovaMIS/login.htm。
还有一台F5020，F5020下的pc均不能访问映射出的地址。

解决方法

公网能够正常访问，说明地址映射正常，F5020下的pc不能访问，还是要检查下防火墙域间策略的配置，pc能正常访问公网，应该是要能ping通222.189.212.194的。

答案来自于 **zhiliao_unRHu**