链滴

华为 USG6000 系列防火墙概览

作者：Gakkiyomi2019

原文链接：https://ld246.com/article/1612436458265

来源网站：链滴

防火墙概览系列又更新了！ 本文会简单介绍下huawei usg6000 的防火墙。

提示

输入 ‘?’ 号 可以命令提示，tab补全命令，quit或者ctrl + z 可以退回上个层级

进入配置configure模式

```
system-view
```

hostname

```
sysname USG6000V2
```

提交配置,用来保存当前配置信息到系统的存储路径中

```
save all
```

获取running配置

```
display current-configuration all
```

interface

```
display interface
```

```
interface GigabitEthernet0/0/0
 undo shutdown
```

原文链接：华为 USG6000 系列防火墙概览

```
 ip binding vpn-instance default
 ip address 192.168.1.60 255.255.255.0
 service-manage http permit
 service-manage https permit
 service-manage ping permit
 service-manage ssh permit
 service-manage snmp permit
 service-manage telnet permit
 service-manage netconf permit
```

Logging

```
display logbuffer
```

address (group)

```
display ip address-set all

ip address-set hello type object
 address 0 11.10.1.0 mask 25

ip address-set ttttt type group
  description asdasd
  address range 10.10.12.2 10.10.12.10
  address address-set addr
  address address-set kkk
  address address-set uuu
  address range 10.10.123.2 10.10.123.10
```

service (group)

```
display ip service-set all

ip service-set fdf type object
    description tgasfasd
    service protocol tcp source-port 0 to 2 destination-port 0 to 65
    service protocol udp source-port 0 to 655 destination-port 0 to 65535
    service protocol tcp source-port 0 to 76 destination-port 88 to 999
    service protocol tcp source-port 666 destination-port 777 to 4564
    service protocol icmp icmp-type 8 9
    service protocol 111
    service protocol icmp icmp-type host-unreachable

ip service-set zxvasfasfsafa type group
    description asdasdsd
    service service-set ad
    service service-set ah
    service service-set bgp
    service service-set discard-tcp
```

zone

```
display zone

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

firewall zone name aaa
 set priority 20
```

application

```
display application user-defined

sa
  user-defined-application name UD_3333
    description ada
    data-model browser-based
    label Productivity-LossEvasiveTunnelingSupports-VideoSocial-ApplicationsNetwork-Storag
Database
    rule name zxc
    protocol tcp
    ip-address 2.2.2.2
    port 3333
    signature context packet direction both plain-string vva field General-Payload
    rule name aaz
    port 6600
    signature context packet direction request regular-expression "aaa?" field General-Payload
    rule name azxc
    ip-address 2.2.2.2
    port 55
    port 66
    port 44
    undo signature
```

policy

```
display security-policy all

security-policy
  rule name dfsd
    description fdsdfd
    source-zone trust
    source-zone local
    destination-zone aaa
    destination-zone untrust
    source-address address-set addr
    source-address address-set asdf
    destination-address address-set addr
    destination-address address-set fangcong
    service ad
    service ah
    application app HTML2JPG_Enterprise_Version
    application category Business_Systems sub-category Auth_Service
```

application app-group dvsd
time-range time1
profile av zxcss
profile ips web_server
action permit
policy logging
session logging
session aging-time 324
long-link enable
long-link aging-time 3243

timeRange

display time-range all

time-range abc
period-range 01:30:00 to 23:00:00 Wed Tue Mon
absolute-range 00:00:00 2019/10/9 to 00:00:00 2019/10/10
absolute-range 00:00:00 2019/10/15 to 00:00:00 2019/10/24

huawei usg Configuring NAT

Static NAT (1对1)

使用static nat 来进行目的地址转换

设备：cisco asa 192.168.1.204

接口：

```
interface Management0/0
 nameif management
 security-level 0
 ip address 192.168.1.204 255.255.255.0
```

```
interface GigabitEthernet0/0
 nameif untrust
 security-level 0
 ip address 172.16.205.1 255.255.255.0
```

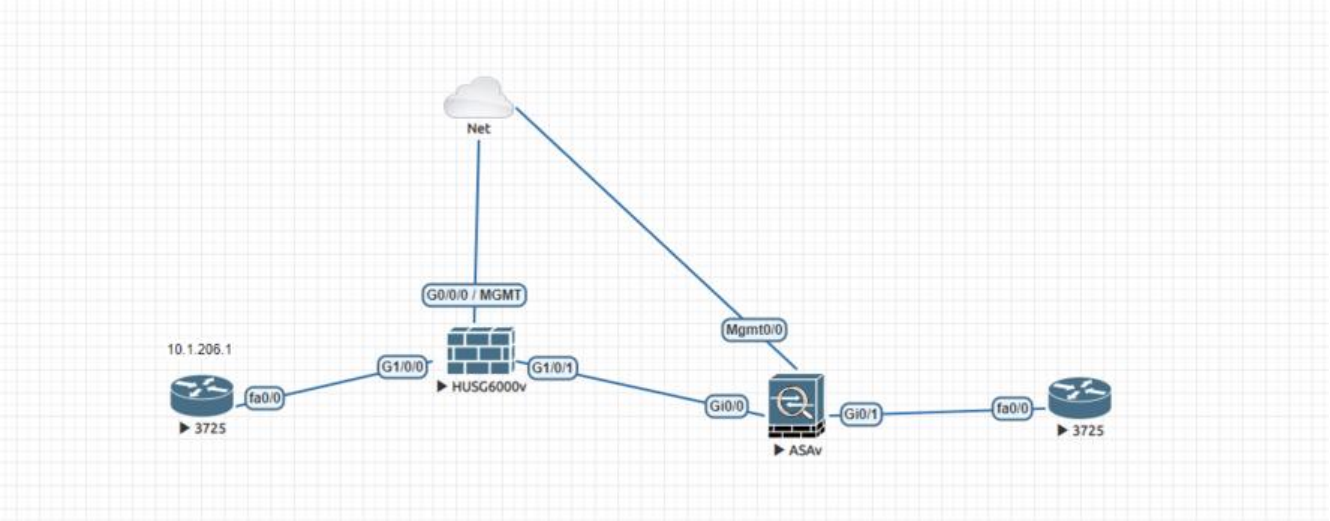
设备:huawei usg 192.168.1.205

接口：

```
interface GigabitEthernet0/0/0
 undo shutdown
 ip binding vpn-instance default
 ip address 192.168.1.205 255.255.255.0
 service-manage http permit
 service-manage https permit
 service-manage ping permit
 service-manage ssh permit
 service-manage snmp permit
 service-manage telnet permit
 service-manage netconf permit
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 10.1.206.254 255.255.255.0
 service-manage http permit
 service-manage https permit
 service-manage ping permit
 service-manage ssh permit
 service-manage snmp permit
 service-manage telnet permit
 service-manage netconf permit
#
```

原文链接：华为 USG6000 系列防火墙概览

拓扑：



华为墙做nat墙

命令：

```
security-policy
rule name untrust_2_dmz_c0dbd
description create by NAP 97e5819c-2c2c-435b-9e29-5e40d8715f9a
source-zone untrust
destination-zone dmz
source-address address-set WS_172.16.205.1_32
destination-address address-set ws_10.1.206.1
service Any
action permit

nat server untrust_2_dmz_b9fe1 global 12.1.214.33 inside 10.1.206.1
```

cisco设备上设置路由:

```
route untrust 12.1.214.0 255.255.255.0 172.16.205.254 1
```

在cisco上ping 12.1.214.33

转换结果

Source NAT

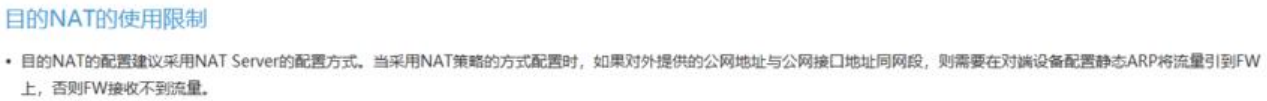
源NAT策略用于实现内网主机使用私网地址访问Internet。系统会将内网主机报文的源IP由私网地址换为公网地址。在配置时，转换前的源地址应选择私网地址或地址组（可多选），转换后的源地址可使用NAT地址池或使用报文出接口的公网IP地址。

```
nat-policy
[USG6000V2-policy-nat]
```

原文链接：华为 USG6000 系列防火墙概览

```
rule name snat1
[USG6000V2-policy-nat-rule-snat1]
description test
[USG6000V2-policy-nat-rule-snat1]
destination-zone untrust
[USG6000V2-policy-nat-rule-snat1]
source-zone trust
[USG6000V2-policy-nat-rule-snat1]
source-address address-set WS_192.168.1.11_32
[USG6000V2-policy-nat-rule-snat1]
destination-address address-set WS_2.3.1.120_32
[USG6000V2-policy-nat-rule-snat1]
service TCP_241
[USG6000V2-policy-nat-rule-snat1]
action nat address-group test2          //test2为地址池里面的地址
[USG6000V2-policy-nat-rule-snat1]
```

Destination NAT



将公网ip12.1.214.33的443端口 映射到私有ip 10.1.206.1的999

```
nat server untrust_2_dmz_b9fe1 protocol tcp  global 12.1.214.33 443 inside 10.1.206.1 9999
```

所以我们会通过nat-server的方式来进行dnat的配置