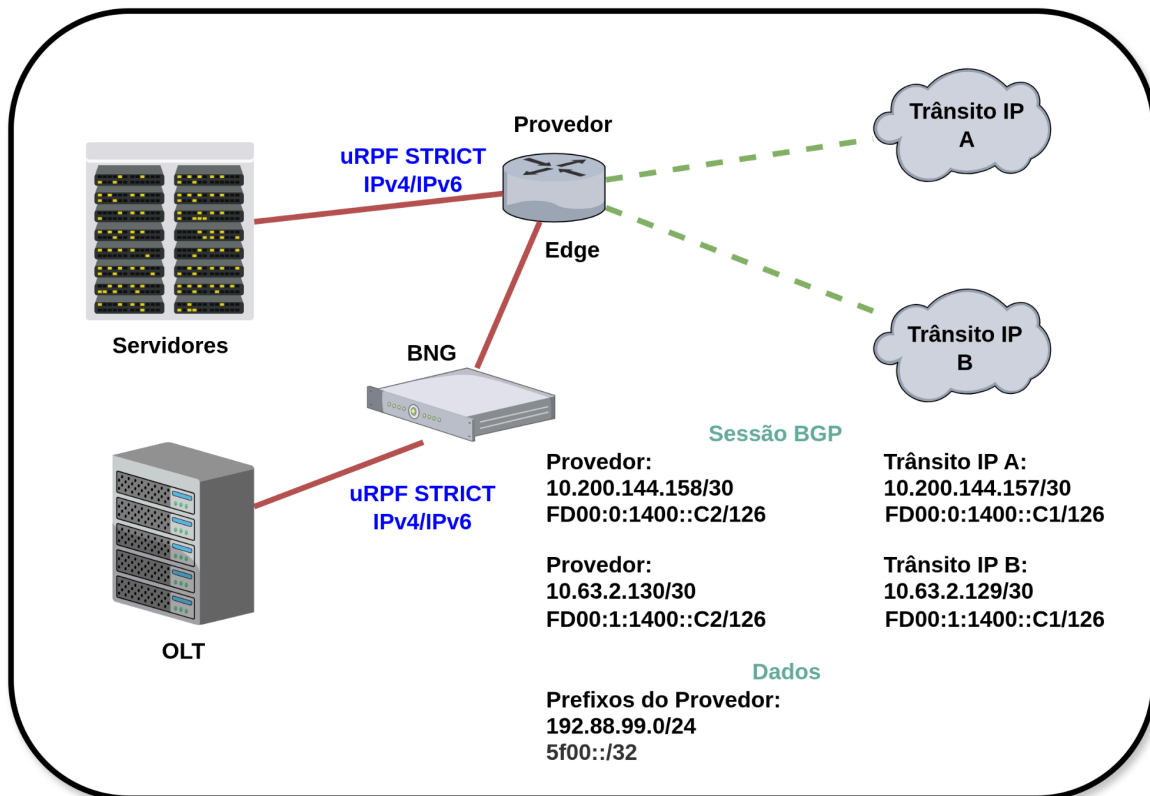


Exemplo de configuração em um **BNG Huawei NE8000**. A configuração abaixo bloqueia **portas de amplificação DDoS** e faz **Gerência de Porta 25**.



```
acl ip-pool ACL_CLIENTES
ip address 192.88.99.0 0.0.0.255
#
acl ipv6-pool ACL_CLIENTESv6
ipv6 address 5f00:: 32
#
acl port-pool ACL_PORTAS_IN
eq 53
eq 161
eq 1900
eq 111
eq 137
eq 10001
eq 5353
eq 389
eq 19
eq 17
eq 11211
eq 3702
eq 69
eq 5683
eq 427
eq 3283
eq 37810
#
```

```
acl port-pool ACL_TCP_IN_BOTNET
eq 4145
eq 5678
#
acl name ACL_DROP_PPPOE_IN advance
rule 1 permit udp destination-pool ACL_CLIENTES destination-port-pool
ACL_PORTAS_IN
#
acl name ACL_IN_BOTNET number 3004
description PORTAS TCP BOTNET IN
rule 1 permit tcp destination-pool ACL_CLIENTES destination-port-pool
ACL_TCP_IN_BOTNET tcp-flag syn
#
acl name ACL_IN_OUT_UDP_123 number 3003
description description ORIGEM NTP
rule 1 permit udp source-pool ACL_CLIENTES source-port eq ntp
rule 2 permit udp source-port eq ntp destination-pool ACL_CLIENTES
#
acl name ACL_IN_UDP_123 number 3002
description BLOQUEIO NTP DE ORIGEM NAO NTP
rule 1 permit udp source-port neq ntp destination-pool ACL_CLIENTES
destination-port eq ntp
#
acl name ACL_OUT_TCP_25 number 3001
description GERENCIA PORTA 25
rule 1 permit tcp source-pool ACL_CLIENTES destination-port eq smtp tcp-flag
syn
#
acl name ACL_PERMIT_PPPOE_IN_EXCECOES advance
description execoes_firewall_in
#
acl ipv6 name ACL_PERMIT_PPPOE_IN_EXCECOESv6 advance
description execoes_firewall_in IPv6
#
acl name ACL_PERMIT_PPPOE_OUT_EXCECOES advance
description Regras de Liberacoes no Firewall
#
acl ipv6 name ACL_PERMIT_PPPOE_OUT_EXCECOESv6 advance
description Regras de Liberacoes no Firewall IPv6
#
acl ipv6 name ACL_DROP_PPPOE_INv6 advance
rule 1 permit udp destination-pool ACL_CLIENTESv6 destination-port eq dns
rule 2 permit udp destination-pool ACL_CLIENTESv6 destination-port eq snmp
rule 3 permit udp destination-pool ACL_CLIENTESv6 destination-port eq 1900
rule 4 permit udp destination-pool ACL_CLIENTESv6 destination-port eq sunrpc
rule 5 permit udp destination-pool ACL_CLIENTESv6 destination-port eq
netbios-ns
rule 6 permit udp destination-pool ACL_CLIENTESv6 destination-port eq 10001
rule 7 permit udp destination-pool ACL_CLIENTESv6 destination-port eq 5353
rule 8 permit udp destination-pool ACL_CLIENTESv6 destination-port eq 389
rule 9 permit udp destination-pool ACL_CLIENTESv6 destination-port eq 19
rule 10 permit udp destination-pool ACL_CLIENTESv6 destination-port eq 17
rule 11 permit udp destination-pool ACL_CLIENTESv6 destination-port eq 11211
rule 12 permit udp destination-pool ACL_CLIENTESv6 destination-port eq 3702
rule 13 permit udp destination-pool ACL_CLIENTESv6 destination-port eq tftp
rule 14 permit udp destination-pool ACL_CLIENTESv6 destination-port eq 5683
rule 15 permit udp destination-pool ACL_CLIENTESv6 destination-port eq 427
rule 16 permit udp destination-pool ACL_CLIENTESv6 destination-port eq 3283
rule 17 permit udp destination-pool ACL_CLIENTESv6 destination-port eq 37810
#
```

```
acl ipv6 name ACL_IN_BOTNETv6 advance
  rule 1 permit tcp destination-pool ACL_CLIENTESv6 destination-port eq
4145 tcp-flag syn
  rule 2 permit tcp destination-pool ACL_CLIENTESv6 destination-port eq
5678 tcp-flag syn
#
acl ipv6 name ACL_IN_OUT_UDP_123v6 advance
  rule 1 permit udp source-pool ACL_CLIENTESv6 source-port eq ntp
  rule 2 permit udp destination-pool ACL_CLIENTESv6 source-port eq ntp
#
acl ipv6 name ACL_IN_UDP_123v6 advance
  rule 1 permit udp destination-pool ACL_CLIENTESv6 source-port neq ntp
destination-port eq ntp
#
acl ipv6 name ACL_OUT_TCP_25v6 advance
  rule 1 permit tcp source-pool ACL_CLIENTESv6 destination-port eq smtp
tcp-flag syn
#
traffic classifier TC_DROP_PPPOE_IN operator or
  if-match acl name ACL_DROP_PPPOE_IN
#
traffic classifier TC_DROP_PPPOE_INV6 operator or
  if-match ipv6 acl name ACL_DROP_PPPOE_INV6
#
traffic classifier TC_IN_BOTNET operator or
  if-match acl name ACL_IN_BOTNET
#
traffic classifier TC_IN_BOTNETv6 operator or
  if-match ipv6 acl name ACL_IN_BOTNETv6
#
traffic classifier TC_IN_OUT_UDP_123 operator or
  if-match acl name ACL_IN_OUT_UDP_123
#
traffic classifier TC_IN_OUT_UDP_123v6 operator or
  if-match ipv6 acl name ACL_IN_OUT_UDP_123v6
#
traffic classifier TC_IN_UDP_123 operator or
  if-match acl name ACL_IN_UDP_123
#
traffic classifier TC_IN_UDP_123v6 operator or
  if-match ipv6 acl name ACL_IN_UDP_123v6
#
traffic classifier TC_OUT_TCP_25 operator or
  if-match acl name ACL_OUT_TCP_25
#
traffic classifier TC_OUT_TCP_25v6 operator or
  if-match ipv6 acl name ACL_OUT_TCP_25v6
#
traffic classifier TC_PERMIT_PPPOE_IN_EXCECOES operator or
  if-match acl name ACL_PERMIT_PPPOE_IN_EXCECOES
#
traffic classifier TC_PERMIT_PPPOE_IN_EXCECOESv6 operator or
  if-match ipv6 acl name ACL_PERMIT_PPPOE_IN_EXCECOESv6
#
traffic classifier TC_PERMIT_PPPOE_OUT_EXCECOES operator or
  if-match acl name ACL_PERMIT_PPPOE_OUT_EXCECOES
#
```



```
traffic classifier TC_PERMIT_PPPOE_OUT_EXCECOESv6 operator or
if-match ipv6 acl name ACL_PERMIT_PPPOE_OUT_EXCECOESv6
#
traffic behavior BH_ACCEPT
#
traffic behavior BH_DROP
deny
#
traffic behavior BH_LIMIT_2Mb
car cir 2000 cbs 2000 green pass red discard
#
traffic policy TP_FIREWALL_GLOBAL_IN
share-mode
statistics enable
classifier TC_PERMIT_PPPOE_IN_EXCECOES behavior BH_ACCEPT precedence 3
classifier TC_PERMIT_PPPOE_IN_EXCECOESv6 behavior BH_ACCEPT precedence 4
classifier TC_IN_UDP_123 behavior BH_DROP precedence 5
classifier TC_IN_UDP_123v6 behavior BH_DROP precedence 6
classifier TC_IN_BOTNET behavior BH_DROP precedence 10
classifier TC_IN_BOTNETv6 behavior BH_DROP precedence 11
classifier TC_IN_OUT_UDP_123 behavior BH_LIMIT_2Mb precedence 15
classifier TC_IN_OUT_UDP_123v6 behavior BH_LIMIT_2Mb precedence 16
classifier TC_DROP_PPPOE_IN behavior BH_DROP precedence 30
classifier TC_DROP_PPPOE_INv6 behavior BH_DROP precedence 31
#
traffic policy TP_FIREWALL_GLOBAL_OUT
share-mode
statistics enable
classifier TC_PERMIT_PPPOE_OUT_EXCECOES behavior BH_ACCEPT precedence 3
classifier TC_PERMIT_PPPOE_OUT_EXCECOESv6 behavior BH_ACCEPT precedence 4
classifier TC_IN_OUT_UDP_123 behavior BH_LIMIT_2Mb precedence 5
classifier TC_IN_OUT_UDP_123v6 behavior BH_LIMIT_2Mb precedence 6
classifier TC_OUT_TCP_25 behavior BH_DROP precedence 25
classifier TC_OUT_TCP_25v6 behavior BH_DROP precedence 26
#
traffic-policy TP_FIREWALL_GLOBAL_IN inbound global
Y
traffic-policy TP_FIREWALL_GLOBAL_OUT outbound global
Y
```