Melhores praticas para ISP usando Juniper MX series

GIOVANELI
CONSULTORIA E TREINAMENTOS

ERROS MAIS COMUNS

- Configurar equipamento em bancada com temperatura não recomendada pelo fabricante que acaba sobreaquecendo e danificando antes de entrar em produção.
- Misturar FONTE AC/DC no mesmo equipamento **Proibido!!!!.**
- Não configura NTP.
- Não configurar TRESHOLDS de ARP para vlans com muita solicitação de ARP.
- Colocar equipamento em produção com versão de software de fabrica.
- Não ajustar os valores de Anti-DDoS para o ambiente.
- Falta de ajuste de filtros e features nos EGP/IGP.
- Ao ter um problema com o equipamento ou uma função não acionar o suporte do fabricante.
- Manter suporte e garantia do equipamento ativo com o fabricante
- Colocar firmwares no equipamento baixados de site duvidosos (abrindo backdoor no equipamento).
- Deixar equipamento com o acesso root ativo via ssh/telnet

Pontos iniciais

- Configurações básicas de login e acesso e variáveis do sistema.
- Proteção de firewall: objetivo é proteger o próprio equipamento de ameaças externas.
- Ajuste dos valores de proteção ANTI DDoS
  - ARP
  - PPPOE
  - DHCPV4
  - DHCPV6
- Configurar variáveis para protocolos de roteamento
  - BFD
  - GRACEFULL RESTART
- Manter equipamento sempre atualizado com a ultima versão Junos SR
- Sempre verificar a temperatura:
  - DA FPC E DA ROUTING ENGINE
  - Do fluxo de ar AFI/AFO

Curso JunoOs – Módulo 1

- Configurando permissões de acesso a caixa.

```
[edit]
root# set system login class ADMINISTRADOR permissions all

[edit]
root# set system login class SUPORTE permissions view

[edit]
root# ...lexandre class ADMINISTRADOR authentication plain-text-password
New password:
Retype new password:

[edit]
root#
```

Curso JunoOs – Módulo 1

- Configurando NTP

```
root# set system ntp boot-server 200.160.0.8

[edit]
root# set system ntp server 200.160.0.8

[edit]
root# set system ntp server 200.189.40.8

[edit]
root#
```

```
root# set system time-zone America/Sao_Paulo

[edit]
root#
```

Curso JunoOs – Módulo 1

- Habilitando ssh

```
root# set system services ssh

[edit]
root#
```

- Negando acesso root através de ssh

```
root# set system services ssh root-login deny

[edit]
```

- Bloqueando acesso ssh através de interfaces de trafego.

```
root# set system services ssh no-tcp-forwarding

[edit]
```

Curso JunoOs – Módulo 1

- Ativando o modo ip enhanced-ip
- Tome muito cuidado pois algumas placas não tem este recurso e no reboot a placa pode parar!

```
root# set system host-name LAB-01

[edit]
root#
```

- Alterando o host-name

```
[edit]
root# set chassis network-services enhanced-ip

[edit]
root#
```

- Ativando LOG

```
root# set system syslog user * any emergency

[edit]
root# set system syslog file messages any notice

[edit]
root# set system syslog file messages authorization info

[edit]
root# set system syslog file interactive-commands interactive-commands any

[edit]
root# set system syslog file LOGS-DE-FIREWALL firewall any
```

Curso JunoOs – Módulo 1

- Ativando SNMP V2

```
root# set snmp client-list 10.1.1.1

[edit]
root# set snmp community comunidadesnmp clients 10.0.0.0/24

[edit]
root#
```

- **Cuidado!!!** *Mesmo você especificando o endereço ip no snmp, existe uma brecha de segurança que permite fazer a coleta dos dados através das interfaces de roteamento, iremos ver nos próximos módulos como resolver isto através dos filtros de interface.*

GIOVANELI
CONSULTORIA E TREINAMENTOS

Curso JunoOs – Módulo 1

- Ativando algumas features:

```
root# set system no-multicast-echo

[edit]
root# set system no-redirects

[edit]
root# set system no-ping-record-route

[edit]
root# set system no-ping-time-stamp

[edit]
root# set system internet-options path-mtu-discovery

[edit]
root# set system internet-options tcp-drop-synfin-set

[edit]
root# set system internet-options ipv6-path-mtu-discovery

[edit]
root# set system ports auxiliary disable

[edit]
root#
```

Curso JunoOs – Módulo 1

- Verificar quais pacotes estão sendo passados na interface

```
root@PROFESSOR-MX0# run monitor traffic interface ge-0/0/0
verbose output suppressed, use <detail> or <extensive> for full protocol decode
Address resolution is ON. Use <no-resolve> to avoid any reverse lookup delay.
Address resolution timeout is 4s.
Listening on ge-0/0/0, capture size 96 bytes

Reverse lookup for 10.255.255.21 failed (check DNS reachability).
Other reverse lookup failures will not be reported.
Use <no-resolve> to avoid reverse lookups on IP addresses.

15:40:00.635839  In arp who-has 10.255.255.21 tell 10.255.255.1
15:40:01.633585  In arp who-has 10.255.255.21 tell 10.255.255.1
15:40:02.702846  In arp who-has 10.255.255.21 tell 10.255.255.1
15:40:10.648291  In arp who-has 10.255.255.21 tell 10.255.255.1
15:40:11.646052  In arp who-has 10.255.255.21 tell 10.255.255.1
15:40:12.646589  In arp who-has 10.255.255.21 tell 10.255.255.1
15:40:13.423432  In IP 10.1.1.200.bootps > 255.255.255.255.bootpc: BOOTP/DHCP, Reply, length 300
15:40:20.659904  In arp who-has 10.255.255.21 tell 10.255.255.1
15:40:21.658324  In arp who-has 10.255.255.21 tell 10.255.255.1
```

Junos Routing Básico - BGP

- Gracefull Restart

```
[edit]
root@PROFESSOR-MX0# set protocols bgp group NETPROFESSOR graceful-restart
```

- Chave de autenticação MD5

```
[edit]
root@PROFESSOR-MX0# set protocols bgp group NETPROFESSOR authentication-key
```

- Descrição

```
[edit]
root@PROFESSOR-MX0# set protocols bgp group NETPROFESSOR description BGP-COM-0-PROFESSOR
```

GIOVANELI
CONSULTORIA E TREINAMENTOS

Junos Routing Básico - OSPF

- Load Balance de pacotes com rotas iguais

```
[edit]
root@vMX-1# set routing-options forwarding-table export load-balance
```

```
[edit]
root@vMX-1# set policy-options policy-statement load-balance then load-balance per-packet
```

JunOs Avançado:

- Firewall e proteção da Router Engine

JunOs Avançado: Firewall protect re

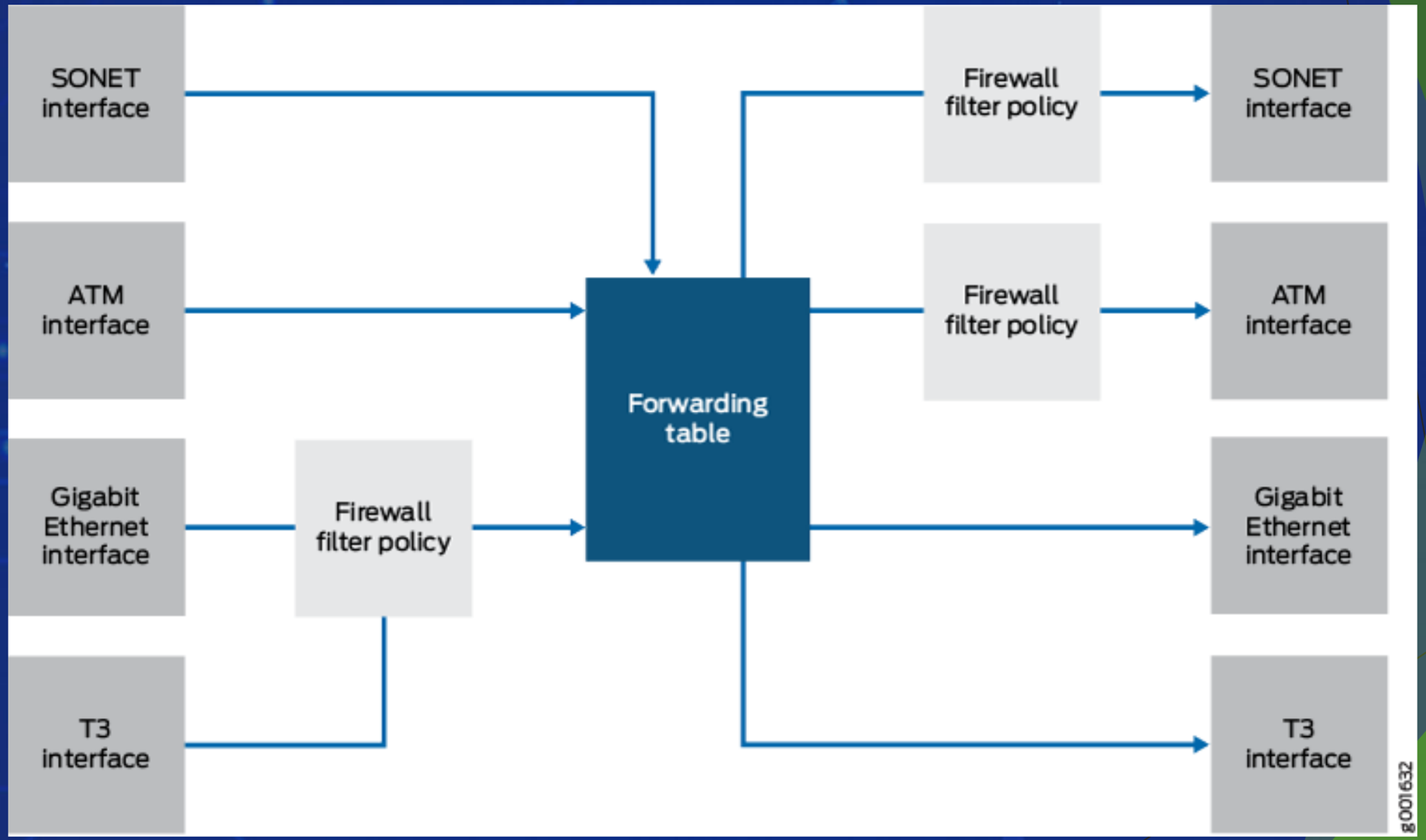
- A ideia da proteção da router engine é evitar que o sitema operaciona seja atacado com floods de pacotes icmp, snmp, tcp syn, entre outros.
- Caso a router engine seja atacada ela pode elevar o uso de cpu e prejudicar os daemons de controle da caixa e até mesmo travar o router.

JunOs Avançado: Firewall protect re

- Regras basicas a serem aplicadas na interface LO0 que responde pela router engine:
  - ICMP FRAGMENTADO
  - SNMP
  - BGP
  - OSPF
  - MPLS
  - LDP
  - NTP
  - ARP (principalmente para as interfaces do IX)
  - Tracertoute
  - Tcp não estabelecidas

GIOVANELI
CONSULTORIA E TREINAMENTOS

JunOs Avançado: Firewall



Firewall protect re

- Diferenças de tipo de firewall no juniper
  - firewall family inet filter
    - Tem a preferencia de ser usado para o input do equipamento por conta das funções de statefull)
  - firewall filter / firewall family inet6 filter -
    - Fowarding ou encaminhamento de pacotes entre interfaces de trafego.
  - Policer = aplica uma politica de velocidade
    - Controle de banda usado para ips, protocolos, arp, etc..
- Formas de firewall nas interfaces
  - set interfaces ge-0/0/0 unit 0 family inet filter input PROTECAO-INTERNET
  - set interfaces ge-0/0/0 unit 30 family inet policer arp INTERFACE-ARP-LIMITA
  - set interfaces lo0 unit 0 family inet filter input PROTECT-RE

GIOVANELI
CONSULTORIA E TREINAMENTOS

- Exemplo de firewall para a ROUTER-ENGINE
- set firewall family inet filter PROTECT-RE term aceita-bgp from prefix-list bgp-peers
- set firewall family inet filter PROTECT-RE term aceita-bgp from protocol tcp
- set firewall family inet filter PROTECT-RE term aceita-bgp from destination-port bgp
- set firewall family inet filter PROTECT-RE term aceita-bgp then accept
- set firewall family inet filter PROTECT-RE term aceita-snmp from prefix-list snmp-servers
- set firewall family inet filter PROTECT-RE term aceita-snmp from protocol udp
- set firewall family inet filter PROTECT-RE term aceita-snmp from destination-port 161
- set firewall family inet filter PROTECT-RE term aceita-snmp then policer limit-1m
- set firewall family inet filter PROTECT-RE term aceita-ntp from prefix-list ntp-servers
- set firewall family inet filter PROTECT-RE term aceita-ntp from prefix-list localhost
- set firewall family inet filter PROTECT-RE term aceita-ntp from protocol udp
- set firewall family inet filter PROTECT-RE term aceita-ntp from port ntp
- set firewall family inet filter PROTECT-RE term aceita-ntp then policer limit-32k

- set firewall family inet filter PROTECT-RE term drop-ntp from protocol udp
- set firewall family inet filter PROTECT-RE term drop-ntp from port ntp
- set firewall family inet filter PROTECT-RE term drop-ntp then discard
- set firewall family inet filter PROTECT-RE term aceita-ospf from protocol ospf
- set firewall family inet filter PROTECT-RE term aceita-ospf then accept
- set firewall family inet filter PROTECT-RE term icmp-fragmentado from is-fragment
- set firewall family inet filter PROTECT-RE term icmp-fragmentado from protocol icmp
- set firewall family inet filter PROTECT-RE term icmp-fragmentado then syslog
- set firewall family inet filter PROTECT-RE term icmp-fragmentado then discard
- set firewall family inet filter PROTECT-RE term aceita-icmp from icmp-type echo-request
- set firewall family inet filter PROTECT-RE term aceita-icmp from icmp-type echo-reply
- set firewall family inet filter PROTECT-RE term aceita-icmp from icmp-type unreachable
- set firewall family inet filter PROTECT-RE term aceita-icmp from icmp-type time-exceeded
- set firewall family inet filter PROTECT-RE term aceita-icmp then policer limit-1m

- set firewall family inet filter PROTECT-RE term aceita-traceroute from protocol udp
- set firewall family inet filter PROTECT-RE term aceita-traceroute from destination-port 33434-33523
- set firewall family inet filter PROTECT-RE term aceita-traceroute then accept
- set firewall family inet filter PROTECT-RE term aceita-ssh from source-address 192.168.88.1
- set firewall family inet filter PROTECT-RE term aceita-ssh from destination-port ssh
- set firewall family inet filter PROTECT-RE term aceita-ssh then policer limit-10m
- set firewall family inet filter PROTECT-RE term aceita-mpls-ldp from protocol tcp port ldp
- set firewall family inet filter PROTECT-RE term aceita-mpls-ldp from protocol udp port ldp
- set firewall family inet filter PROTECT-RE term aceita-mpls-ldp then accept
- set firewall family inet filter PROTECT-RE term tcp-estabelecidas from protocol tcp
- set firewall family inet filter PROTECT-RE term tcp-estabelecidas from source-port ssh
- set firewall family inet filter PROTECT-RE term tcp-estabelecidas from source-port bgp
- set firewall family inet filter PROTECT-RE term tcp-estabelecidas from tcp-established
- set firewall family inet filter PROTECT-RE term tcp-estabelecidas then accept
- set firewall family inet filter PROTECT-RE term descarta-resto then syslog
- set firewall family inet filter PROTECT-RE term descarta-resto then discard

JunOs Avançado: Firewall protect re (arp)

- Para o ptt de são paulo
  - set firewall policer INTERFACE-ARP-LIMITA if-exceeding bandwidth-limit 512k
  - set firewall policer INTERFACE-ARP-LIMITA if-exceeding burst-size-limit 64k
  - set firewall policer INTERFACE-ARP-LIMITA then discard

- Politicas de firewall contra abuso na rede do ISP :
  - set firewall filter PROTECAO-INTERNET term 10 from prefix-list ACEITA-CONSULTA-REVERSA
  - set firewall filter PROTECAO-INTERNET term 10 from destination-port 53
  - set firewall filter PROTECAO-INTERNET term 10 the policer LIMIT-2M
  - set firewall filter PROTECAO-INTERNET term 10 then accept
  - set firewall filter PROTECAO-INTERNET term 20 from protocol udp
  - set firewall filter PROTECAO-INTERNET term 20 from destination-port snmp
  - set firewall filter PROTECAO-INTERNET term 20 from destination-port ntp
  - set firewall filter PROTECAO-INTERNET term 20 from destination-port 1900
  - set firewall filter PROTECAO-INTERNET term 20 from destination-port domain
  - set firewall filter PROTECAO-INTERNET term 20 from destination-port netbios-ns
  - set firewall filter PROTECAO-INTERNET term 20 from destination-port netbios-ssn
  - set firewall filter PROTECAO-INTERNET term 20 from destination-port netbios-dgm
  - set firewall filter PROTECAO-INTERNET term 20 from destination-port 1434
  - set firewall filter PROTECAO-INTERNET term 20 from destination-port 69
  - set firewall filter PROTECAO-INTERNET term 20 from destination-port 111
  - set firewall filter PROTECAO-INTERNET term 20 from destination-port 2049
  - set firewall filter PROTECAO-INTERNET term 20 from destination-port 3133
  - set firewall filter PROTECAO-INTERNET term 20 from destination-port 0
  - set firewall filter PROTECAO-INTERNET term 20 then discard

- set firewall filter PROTECAO-INTERNET term 25 from prefix-list BLOQUEIA-SERVIDORES
- set firewall filter PROTECAO-INTERNET term 25 then discard
- set firewall filter PROTECAO-INTERNET term icmp-fragmentado from is-fragment
- set firewall filter PROTECAO-INTERNET term icmp-fragmentado from protocol icmp
- set firewall filter PROTECAO-INTERNET term icmp-fragmentado then discard
- set firewall filter PROTECAO-INTERNET term 30 from protocol tcp
- set firewall filter PROTECAO-INTERNET term 30 from destination-port ssh
- set firewall filter PROTECAO-INTERNET term 30 from destination-port telnet
- set firewall filter PROTECAO-INTERNET term 30 from destination-port ftp
- set firewall filter PROTECAO-INTERNET term 30 from destination-port 9001
- set firewall filter PROTECAO-INTERNET term 30 then discard
- set firewall filter PROTECAO-INTERNET term 35 from prefix-list BLOQUEIA-AS
- set firewall filter PROTECAO-INTERNET term 35 then discard
- set firewall filter PROTECAO-INTERNET term aceita-o-resto then accept

GIOVANELI
CONSULTORIA E TREINAMENTOS

Exemplos de anti-ddos

- set system ddos-protection protocols pppoe aggregate bandwidth 10000
- set system ddos-protection protocols pppoe padi bandwidth 10
- set system ddos-protection protocols pppoe padi burst 10
- set system ddos-protection protocols pppoe padi recover-time 1
- set system ddos-protection protocols dhcpv4 aggregate bandwidth 100000
- set system ddos-protection protocols dhcpv4 aggregate burst 100000
- set system ddos-protection protocols dhcpv4 discover bandwidth 100000
- set system ddos-protection protocols dhcpv4 discover burst 10000
- set system ddos-protection protocols dhcpv4 discover recover-time 10
- set system ddos-protection protocols dhcpv4 offer fpc 1 bandwidth-scale 80
- set system ddos-protection protocols dhcpv4 offer fpc 1 burst-scale 75
- set system ddos-protection protocols dhcpv4 offer bypass-aggregate
- set system ddos-protection protocols dhcpv4 offer priority médium
- set system ddos-protection protocols dhcpv6 aggregate bandwidth 100
- set system ddos-protection protocols dhcpv6 aggregate burst 100
- set system ddos-protection protocols dhcpv6 solicit bandwidth 100
- set system ddos-protection protocols dhcpv6 solicit burst 100
- set system ddos-protection protocols dhcpv6 solicit recover-time 10


```
[edit]
giovaneli@                  # run show ddos-protection protocols icmp
Packet types: 1, Modified: 0, Received traffic: 1, Currently violated: 0
Currently tracked flows: 0, Total detected flows: 0
* = User configured value

Protocol Group: ICMP

  Packet type: aggregate (Aggregate for all ICMP traffic)
    Aggregate policer configuration:
      Bandwidth:          20000 pps
      Burst:              20000 packets
      Recover time:       300 seconds
      Enabled:            Yes
    Flow detection configuration:
      Detection mode: Automatic  Detect time:  3 seconds
      Log flows:      Yes        Recover time: 60 seconds
      Timeout flows:  No         Timeout time: 300 seconds
      Flow aggregation level configuration:
        Aggregation level   Detection mode  Control mode  Flow rate
        Subscriber          Automatic       Drop          10 pps
        Logical interface   Automatic       Drop          10 pps
        Physical interface  Automatic       Drop          20000 pps
    System-wide information:
      Aggregate bandwidth is never violated
      Received:  216133              Arrival rate:     0 pps
      Dropped:   0                   Max arrival rate: 43 pps
    Routing Engine information:
      Bandwidth: 20000 pps, Burst: 20000 packets, enabled
      Aggregate policer is never violated
      Received:  216133              Arrival rate:     0 pps
      Dropped:   0                   Max arrival rate: 44 pps
        Dropped by individual policers: 0
    FPC slot 0 information:
      Bandwidth: 100% (20000 pps), Burst: 100% (20000 packets), enabled
      Aggregate policer is never violated
      Received:  216133              Arrival rate:     0 pps
      Dropped:   0                   Max arrival rate: 43 pps
        Dropped by individual policers: 0
        Dropped by flow suppression:    0
```

GIOVANELI
CONSULTORIA E TREINAMENTOS

```
giovaneli[redacted]# run show ddos-protection protocols arp
Packet types: 1, Modified: 0, Received traffic: 1, Currently violated: 0
Currently tracked flows: 0, Total detected flows: 0
* = User configured value

Protocol Group: ARP

  Packet type: aggregate (Aggregate for all arp traffic)
    Aggregate policer configuration:
      Bandwidth:          20000 pps
      Burst:              20000 packets
      Recover time:       300 seconds
      Enabled:            Yes
    Flow detection configuration:
      Detection mode: Automatic  Detect time:  3 seconds
      Log flows:      Yes        Recover time: 60 seconds
      Timeout flows:  No         Timeout time: 300 seconds
      Flow aggregation level configuration:
        Aggregation level   Detection mode  Control mode  Flow rate
        Subscriber          Automatic       Drop          10 pps
        Logical interface   Automatic       Drop          10 pps
        Physical interface  Automatic       Drop          20000 pps
    System-wide information:
      Aggregate bandwidth is never violated
      Received:  8477100              Arrival rate:     9 pps
      Dropped:   0                    Max arrival rate: 57 pps
    Routing Engine information:
      Bandwidth: 20000 pps, Burst: 20000 packets, enabled
      Aggregate policer is never violated
      Received:  8477126              Arrival rate:     9 pps
      Dropped:   0                    Max arrival rate: 51 pps
        Dropped by individual policers: 0
    FPC slot 0 information:
      Bandwidth: 100% (20000 pps), Burst: 100% (20000 packets), enabled
      Aggregate policer is never violated
      Received:  8477100              Arrival rate:     9 pps
      Dropped:   0                    Max arrival rate: 57 pps
        Dropped by individual policers: 0
        Dropped by flow suppression:    0
```

GIOVANELI
CONSULTORIA E TREINAMENTOS

```
[edit]
giovaneli@[illegible]# run show ddos-protection protocols violations
Packet types: 235, Currently violated: 0

[edit]
```

- Atenção!!!
  - Todos estes firewall se não for aplicado a uma interface não importa qual tipo ela seja , só servira de enfeite de natal.

GIOVANELI
CONSULTORIA E TREINAMENTOS

Duvidas ?

scansource

GIOVANELI
CONSULTORIA E TREINAMENTOS

GIOVANELI
CONSULTORIA E TREINAMENTOS

ALEXANDRE GIOVANELI
CEO

+55 31 9 **8255-5555**
www.giovaneli.net