MANRS KINDNS TOP TESTE OS PADRÕES

Recomendações de segurança para provedores

MANRS KINDNS TOP TESTE OS PADRÕES

Durante anos ouvimos falar em crescimento do **DDoS** no mundo, aumento de **Botnets** e incidentes com bordas desprotegidas e mal configuradas. O que podemos e devemos fazer para mudar este cenário?

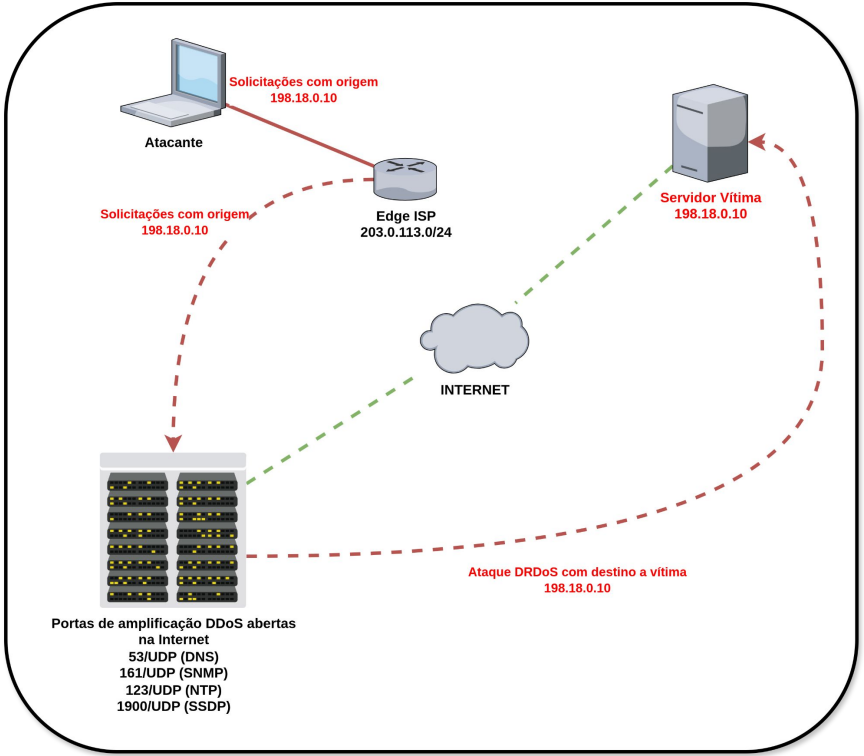
Pontos que abordaremos nesta palestra:

- **BCP38** (RFC2827) e **BCP84** (RFC3704): como ativar o anti-spoofing nos concentradores e bordas da rede, usando **uRPF (Unicast Reverse Path Forwarding)** e outros filtros.
- **Hardening de CPE(s)**: como configurar as CPEs do provedor no cliente sem deixar portas abertas desnecessariamente, com senha única e forte, etc.
- **Hardening de Borda** (RFC6192): como melhorar a segurança dos nossos Edges.

MANRS KINDNS TOP TESTE OS PADRÕES

BCP38 / BCP84

Quando falamos de **BCP38 / BCP84**, estamos falando de **filtros anti-spoofing**. O **spoofing** é o maior facilitador para **ataques DDoS** que é a principal dor de cabeça dos Provedores de Internet atualmente. Mas por que isso acontece? Existe solução para combater o **spoofing**?



BCP38 / BCP84 falam da implementação de um recurso chamado **uRPF (Unicast Reverse Path Forwarding)**. Ele existe como opção para ser habilitado nos principais vendors e dentre as modalidades podemos nos atentar em **strict** e **loose**.

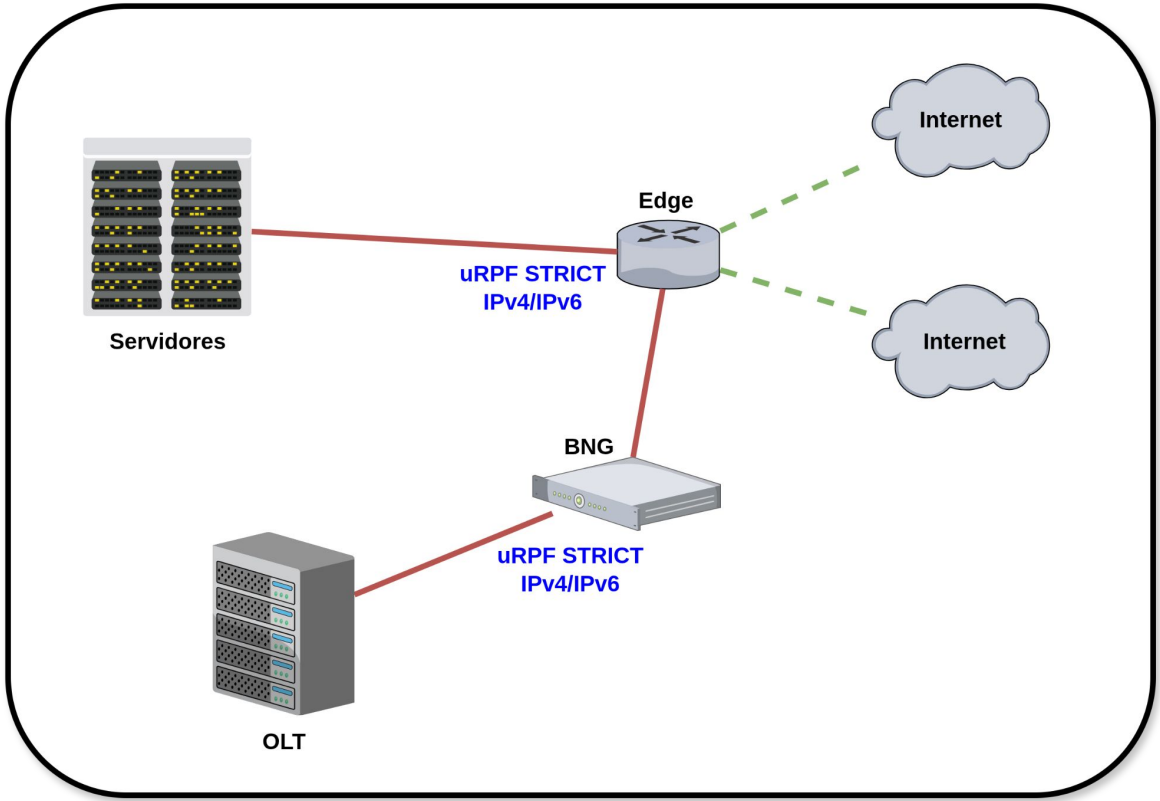
O modo **strict** é o mais rigoroso pois checa se o pacote **recebido pela interface**, **tem retorno de resposta por ela mesma**. Em caso negativo o pacote é descartado na hora.

O modo **loose** é mais permissivo, ele checa apenas se o pacote tem rota de retorno na **FIB (Forwarding Information base)**, desprezando a rota default. Em caso positivo, o pacote é liberado para seguir.

Ambos os modos devem ser aplicados para as famílias **IPv4** e **IPv6**.

Costuma-se utilizar o modo **strict** nos **BNG(s)/B-RAS(s)** e o modo **loose** nos **Edges**. Isso porque o modo **strict** não funciona corretamente com **tráfego assimétrico** e o modo **loose** consegue trabalhar com ambiente **multihomed**, pois consulta apenas a tabela **FIB do roteador**. É possível usar **modo strict** em ambiente **multihomed**? Sim é possível, mas o **uRPF** precisa estar habilitado somente na interface do edge cujo **tráfego não seja assimétrico**.

Neste diagrama podemos visualizar e entender onde podemos aplicar cirurgicamente o **uRPF por interface**. Não habilite o **uRPF globalmente na caixa**. Pode causar anomalias imprevisíveis de acesso.



Veremos alguns exemplos de como fazer a configuração para alguns vendors:

Huawei:

```
interface GigabitEthernet0/0/0
    ip urpf <strict/loose>
    ipv6 urpf <strict/loose>
```

Juniper:

```
family inet {
     rpf-check;
}
family inet6 {
     rpf-check;
}
```

Cisco:

```
ip verify unicast reachable-via rx allow-default
ipv6 verify unicast source reachable-via rx allow-default
```

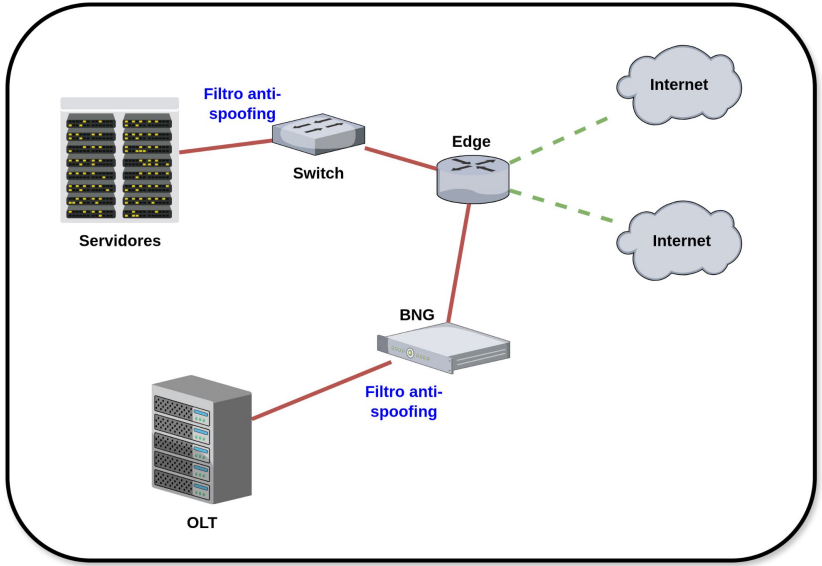
Mikrotik RouterOS:

```
/ip settings set rp-filter=strict
/ip settings set rp-filter=loose
```

No **RouterOS** não existe implementação, até o momento, de **uRPF** para **IPv6**, então a opção é através de **ACL** bloqueando pacotes cuja origem não seja dos prefixos IP do seu ASN. Para **ITP**(s) **Internet Transit Providers**, isso se torna mais complexo de se fazer sem a implementação do **uRPF**.
Outros exemplos para outros fabricantes pode ser encontrado aqui: https://manrs.org/netops/guide/#4.3.2.

Quando o **uRPF** não puder ser utilizado devido a falta de implementação pelo fabricante do equipamento, podemos recorrer ao bom e velho filtro de pacotes. Contudo se você for não só um **ISP** (**Internet Service Provider**) mas também um **ITP** (**Internet Transit Provider**), sinal que você faz trânsito para outros AS(s) e aplicar esse tipo de controle na **borda** pode ser mais complicado.

Para esses casos de **ITP** pode ser mais apropriado aplicar os **filtros anti-spoofing** em equipamentos mais próximos do cliente como os **BNG**(s) e equipamentos que atendam serviços específicos da Operação como por exemplo a rede de servidores. Na borda pode ser aplicado filtros para **BOGONs**.



Cada fabricante possui sua própria **sintaxe** para aplicar os filtros de pacotes no equipamento. Aqui passaremos as regras de forma conceitual, que servirão para todos os casos precisando apenas converter para a sintaxe do seu equipamento.

- Bloquear pacotes de qualquer origem IPv4 ou IPv6 que não pertença ao seu **ASN** e que não esteja sendo usado no seu **CGNAT** com destino a **Internet**. Pode ser feito com segurança no seu **BNG** e equipamentos dentro do domínio do seu AS.

- Bloquear **BOGONs IPv4** e **IPv6** na borda, antes da saída para a **Internet**.

- Bloquear pacotes de **origem IP** pertencentes ao **seu ASN** sendo recebidos da **Internet** em sua borda.

Uma boa referência com configurações para alguns vendors como **Huawei**, **Juniper**, **Nokia** e **softrouters** como **BIRD**, **FRR**, **VyOS**, pode ser encontrada aqui: https://bgpfilterguide.nlnog.net/guides/bogon_prefixes/

Segue anexo **filtros_edge_huawei.pdf** com exemplo de **anti-spoofing** em regras de ACL(s). Reforçando que o uso do uRPF é mais simples de se implementar em diversos fabricantes de equipamentos.

IPv4 Prefixo	Descrição
0.0.0.0/8	RFC 1122 – “this” network
10.0.0.0/8	RFC 1918 – private space
100.64.0.0/10	RFC 6598 – carrier-grade NAT space
127.0.0.0/8	RFC 1122 – localhost
169.254.0.0/16	RFC 3927 – link-local
172.16.0.0/12	RFC 1918 – private space
192.0.2.0/24	RFC 5737 – TEST-NET-1
192.88.99.0/24	RFC 7526 – 6to4 anycast relay
192.168.0.0/16	RFC 1918 – private space
198.18.0.0/15	RFC 2544 – benchmarking
198.51.100.0/24	RFC 5737 – TEST-NET-2
203.0.113.0/24	RFC 5737 – TEST-NET-3
224.0.0.0/4	Multicast
240.0.0.0/4	Reserved

IPv6 Prefixo	Descrição
0100::/64	RFC 6666 – Discard-Only
2001:2::/48	RFC 5180 – BMWG
2001:10::/28	RFC 4843 – ORCHID
2001:db8::/32	RFC 3849 – Documentation
2002::/16	RFC 7526 – 6to4 anycast relay
3ffe::/16	RFC 3701 – old 6bone
3fff::/20	RFC 9637 – Documentation
5f00::/16	RFC 9602 – SRv6 SIDs
fc00::/7	RFC 4193 – unique local unicast
fe80::/10	RFC 4291 – link-local unicast
fec0::/10	RFC 3879 – old site-local unicast
ff00::/8	RFC 4291 – multicast

Como eu testo? A **CAIDA** tem um programa específico para teste de spoofing chamado **Spoofer** e as instruções de como baixar, instalar e executar podem ser encontradas nessa URL: https://www.caida.org/projects/spoofer/

O **Spoofer** pode ser rodado no **Windows**, **macOS** e **GNU/Linux**. Para um teste mais correto é bom que se faça o teste de um equipamento com **IPv4 público** e **IPv6 global**, **sem passar por CGNAT**.

Em anexo o arquivo **spoofer.pdf** onde eu demonstro como instalar o **spoofer** em um **Debian GNU/Linux** e como colocar ele para gerar um relatório semanal na **CAIDA**, que servirá para o **MANRS**.

Concluindo: a configuração do **uRPF** se torna mais simples que a criação de **ACL**s e também menos onerosa para o processamento do equipamento. Contudo a aplicação dos **filtros para bloqueio de BOGONs na borda**, pode ser considerado complementar à segurança.

Um projeto muito interessante e gratuito é o **Bogons Networks da Team Cymru**. Você solicita uma sessão **BGP IPv4** e **IPv6** com eles através desse link: https://www.team-cymru.com/ty/bogons-networks

Uma vez a sessão BGP estabelecida, eles enviam todas as listas de prefixos considerados BOGONs tanto de IPv4, quanto de IPv6 e com isso podem ser geradas regras para dropar esses prefixos na caixa, como por exemplo apontando-os para **192.0.2.1**.

Aqui você encontra diversos exemplos de configuração para vários fabricantes:
https://www.team-cymru.com/bogon-reference-bgp

MANRS KINDNS TOP TESTE OS PADRÕES

Hardening de CPE(s)

CPE(s) com portas de serviços abertas podem ser um convite para atacantes explorarem alguma vulnerabilidade e comprometer o equipamento do Provedor de Internet. Pode causar danos financeiros e pessoais ao cliente e se tornar uma ameaça à **Infraestrutura da Operação**.

A proteção pode ser melhorada em 3 pontos:

- Na **CPE** envolvendo configurações de preset para os provisionamentos nos clientes.
- **ACL**(s) de bloqueio de **Portas de Amplificação DDoS** nos BNG(s) com destino os clientes.
- Troca do **usuário** e **senha padrões** por credenciais mais fortes.

O melhor cenário mas dificilmente encontrado nos **Provedores de Internet** brasileiros, é a **homogeneidade** de **equipamentos/vendors** de OLT(s) e ONT(s) numa mesma rede. Nesse cenário seria possível utilizar o **OMCI** (**Open Management and Control Interface**) do fabricante para deixar programado o provisionamento das ONT(s) de maneira que fique mais protegido e com serviços fechados para a Internet. Mas em um ambiente **heterogêneo** de OLT(s) e ONT(s) e por não ser uma linguagem padrão entre fornecedores, isso se torna inviável.

Com o **OMCI** podemos definir algumas configurações padrões para serem aplicadas nos provisionamentos das ONT(s) como por exemplo:

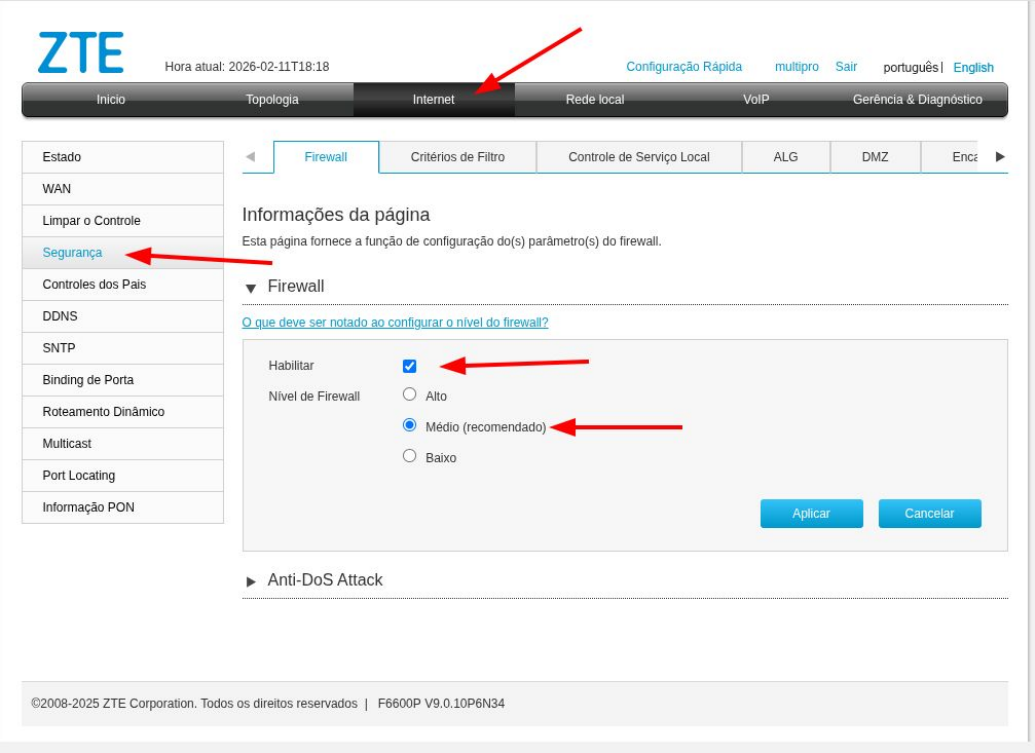
- Bloqueio de acessos externos com **origem** a **Internet** e o **destino** a **CPE do assinante** através da **WAN** do equipamento. Permitindo acesso apenas de uma rede de gerência do Provedor.

- Habilitar a função **Firewall** da CPE, bloqueando acessos com origem a **Internet** e o destino sendo a **rede interna** do assinante.

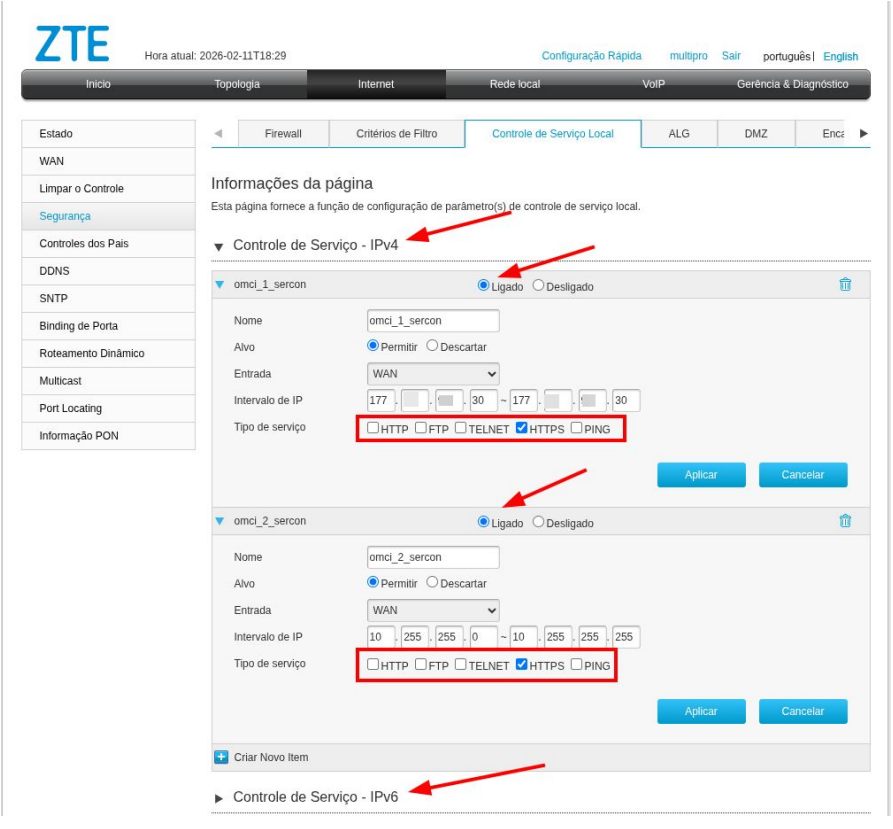
- Desabilitar serviços não necessários na **CPE** como: **DNS**, **Telnet**, **SSH**, etc.

Implementado essas configurações você estará mais protegido contra **vulnerabilidades** que possam vir a surgir para um determinado **modelo/fabricante** de equipamento. A proteção visa também impedir o uso do equipamento mal configurado em ataques de **DRDoS**.

Esse é um exemplo de configuração manual de uma **ONT ZTE F6600P**, onde podemos habilitar o **Firewall** no **nível médio** que já faz o bloqueio de acesso de tudo que vier da Internet, para a **CPE** e para o assinante. Tanto em **IPv4** quanto em **IPv6**. Pode ser configurado como padrão via **OMCI**.



Ainda na **ONT ZTE F6600P** podemos configurar por família de protocolo **IPv4** e **IPv6**, quais **serviços** ficarão habilitados e quais **prefixos** poderão acessá-los. Também pode ser configurado automaticamente via **OMCI**.



Para termos certeza que não existem portas de serviço abertas na **CPE** podemos usar um programa chamado **nmap** e que pode ser instalado em qualquer sistema. O teste deve ser feito como se você estivesse vindo da **Internet**. Por exemplo se o IP da **CPE** conectada fosse **198.18.0.10**.

```
# nmap -p- -sS -sU -P0 -T4 198.18.0.10
```

```
┌─[root@DPAT-01-STZ]─[~]─[22:07:42]
└──╼ # nmap -p- -sS -sU -P0 -T4 177.
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-11 22:07 -03
Nmap scan report for 177-1                    .net.br (177.    )
Host is up (0.023s latency).
Not shown: 64668 filtered tcp ports (no-response), 866 filtered tcp ports (host-unreach), 65522 open|filtered udp ports (no-response)
PORT      STATE  SERVICE
58000/tcp open   unknown
4000/udp  closed icq
4001/udp  closed newoak
4002/udp  closed pxc-spvr-ft
4003/udp  closed pxc-splr-ft
4004/udp  closed pxc-roid
4005/udp  closed pxc-pin
4006/udp  closed pxc-spvr
4007/udp  closed pxc-splr
4008/udp  closed netcheque
4009/udp  closed chimera-hwm
4010/udp  closed samsung-unidex
4011/udp  closed altserviceboot
4012/udp  closed pda-gate

Nmap done: 1 IP address (1 host up) scanned in 846.63 seconds
┌─[root@DPAT-01-STZ]─[~]─[22:21:50]
└──╼ #
```

O comando acima fará um scan **TCP** e **UDP** no **IP 198.18.0.10** e o resultado não pode mostrar portas **open** (**abertas**), somente portas **closed** e **filtered**.

Uma vez validado o setup basta manter dentro do processo de provisionamento das CPE(s).

Quando o uso do **OMCI** se torna impossibilitado, uma outra maneira complementar mais invasiva pode ser aplicada nos BNG(s) usando **filtros de pacotes**. Estes filtros bloqueiam tentativas de conexão originadas da **Internet** para portas consideradas perigosas e de amplificação DDoS com destino o cliente final.

Em anexo temos o arquivo **filtros_bng_huawei.pdf** com exemplo de filtros para bloqueio de **portas de amplificação DDoS** com destino nossos clientes.

Exemplo de configuração **OMCI** da ZTE para a ONT modelo **ZTE-F6600P** como **router**:

```
terminal length 0
conf t
interface gpon olt-1/{slot}/{pon}
onu {onu} type ZTE-F6600P sn {id}
exit
interface gpon onu-1/{slot}/{pon}:{onu}
name {description}
vport-mode manual
tcont 1 name INTERNET profile 1G
gemport 1 name INTERNET tcont 1
vport 1 map-type vlan
vport-map 1 1 vlan {vlan}
exit
interface vport-1/{slot}/{pon}.{onu}:1
service-port 1 user-vlan {vlan} vlan {vlan}
exit
```

Exemplo de configuração **OMCI** da ZTE para a ONT modelo **ZTE-F6600P** como **router**:

```
pon-onu-mng gpon onu-1/{slot}/{pon}:{onu}
service INTERNET gemport 1 vlan {vlan}
wan-ip ipv4 mode pppoe auth chap username {pppoe_login} password {pppoe_password} vlan-profile {vlan} host 1
firewall enable level medium
security-mgmt 1 state enable mode forward protocol web https
security-mgmt 1 start-src-ip 192.88.99.30 end-src-ip 192.88.99.30
security-mgmt 2 state enable mode forward protocol web https tr069
security-mgmt 2 start-src-ip 10.255.255.0 end-src-ip 10.255.255.255
tr069-mgmt 1 state unlock acs http://acs.provedor.net.br:7547/ validate basic username cpe password   senha_forte
ssid ctrl wifi_0/1 user-isolation disable
ssid ctrl wifi_0/5 user-isolation disable
ssid auth wpa wifi_0/1 auth-algrithm wpa2-psk encrypt-algrithm aes key {onu_wifi_password}
ssid auth wpa wifi_0/5 auth-algrithm wpa2-psk encrypt-algrithm aes key {onu_wifi_password5}
ssid ctrl wifi_0/1 name {onu wifi ssid}
ssid ctrl wifi_0/5 name {onu_wifi_ssid5}
end
sleep=15
```

MANRS KINDNS TOP TESTE OS PADRÕES

Hardening de Borda RFC6192

Assim como temos que ter cuidado com nossas CPE(s), precisamos proteger nossas bordas também (**Controle Plane**). Até mesmo os equipamentos mais robustos que utilizam **ASIC**s(Application Specific Integrated Circuits) podem ficar sobrecarregados se não forem bem protegidos. Ações que podemos tomar:

- Desabilitar qualquer serviço na caixa, que não seja necessário.
- Criar um filtro de pacotes para proteger o acesso ao equipamento. **Por padrão tudo bloqueado**.
- Liberar para o Controle Plane **ICMP** e **ICMPv6** com **rate-limit de 500Kbps**.
- Permitir tráfego origem **Link-Local fe80::/10**.
- Permitir tráfego **DNS**, **SNMP**, **NTP**, **SSH** e **TACACS/Radius** somente de serviços seus e **Rede de Gerência**.
- Liberar **portas de serviço** para acesso somente de **peers** necessários. Um exemplo prático é a porta **179/TCP** (**BGP**). Esta porta estando exposta para a **Internet**, pode ser atacada e sofrer um **DoS** (**Denial of Service**) causando flaps nas sessões BGP.
- Dar preferência ao uso de **IPs privados nas sessões BGP** com as **Operadoras de Trânsito IP**. Diminui a superfície de ataque e protege mais sua borda de ataques externos.
- Passar um scanner com o **nmap** para checar se existe alguma porta aberta na sua borda.

Seguimos com uma configuração em anexo em **filtros_edge_huawei.pdf**.

MANRS KINDNS TOP TESTE OS PADRÕES

Parceiros:

3R SOLUTIONS

+

Marcelo Gondim

DÚVIDAS?

MANRS

KINDNS

TOP
TESTE OS PADRÕES