SOLICITAÇÃO DE ENCAMINHAMENTO DE PORTA E DMZ

Agora entramos nos **problemas da Camada 4 (Transporte)**, que no suporte técnico estão, na prática, ligados a:

- **Encaminhamento de portas (Port Forward / Virtual Server)**
- **DMZ (Zona Desmilitarizada)**

Esses recursos são usados quando o cliente precisa **acessar um equipamento da rede interna a partir da internet**, como:

- Câmeras
- DVRs
- Servidores web
- Sistemas internos
- Roteadores (MikroTik, por exemplo)

Cenário do cliente (situação real)

O cliente possui um equipamento na rede interna e acessa esse equipamento localmente:

- Porta **8091** → acesso via navegador (WebFig)
- Porta **8291** → acesso via aplicativo (Winbox)

Localmente isso funciona, mas o cliente quer acessar **de fora da rede**, pela internet. Para isso, **o roteador/ONT precisa saber para qual equipamento interno enviar essas conexões**. É aqui que entram o **Port Forward** e o **DMZ**.

Antes de qualquer configuração (passo mais importante)

🔴 **O cliente precisa ter IP público na ONT**.

- **Com IP público** → Port Forward e DMZ funcionam
- **Com CGNAT** → NÃO funciona (nem Port Forward, nem DMZ)
- **IP dinâmico** → Funciona, mas o IP muda (precisa de DDNS)

- **IP fixo** → Funciona perfeitamente

Sem IP público, **não adianta configurar nada**.

Encaminhamento de portas (Port Forward)

O que é Port Forward?

É uma regra que diz:

"Quando alguém acessar minha internet pela porta X, envie isso para o equipamento Y, na porta Z."

Como configurar (lógica, não decorar ONT)

Os nomes mudam conforme a ONT, mas o conceito é sempre o mesmo (Pode aparecer como *Virtual Server*, *Port Forward*, *NAT Forwarding*).

Campos importantes:

1. **Interface**
    - WAN (ou Internet)
2. **External Port (porta externa)**
    - Porta usada na internet
    - Exemplo: **8091**
3. **Internal IP**
    - IP do equipamento interno
    - ⚠️ **Deve ser IP fixo**
    - Exemplo: 192.168.1.100
4. **Internal Port**
    - Porta que o serviço usa internamente
    - Exemplo: **8091**
5. **Protocol**

- TCP / UDP / ALL
- Em dúvida, use **ALL**

6. **Habilitar / Salvar**

👉 Isso resolve quando o cliente precisa abrir **poucas portas específicas**.

E o DMZ? O que é e por que usar?

O que é DMZ?

DMZ significa:

"Tudo que vier da internet e não tiver regra, envie direto para um único equipamento."

Ou seja:

- O equipamento em DMZ recebe **todas as portas**
- Ele fica **exposto à internet**

Quando usar DMZ?

O DMZ é útil quando:

- O cliente usa **muitas portas**
- O sistema é complexo
- O cliente não sabe quais portas precisa abrir
- É um teste rápido para validar se o problema é NAT

⚠️ **DMZ não é recomendado para segurança**, mas é funcional.

Como habilitar o DMZ

1. Acesse as configurações de **NAT / DMZ**
2. Informe o **IP interno do equipamento**
    - ⚠️ **IP fixo obrigatório**
3. Habilite o DMZ

4. Salve

A partir disso, **todo tráfego externo será enviado para esse equipamento**.

Diferença clara entre Port Forward e DMZ

Port Forward	**DMZ**
Abre portas específicas	Abre todas as portas
Mais seguro	Menos seguro
Ideal para poucos serviços	Ideal para muitos serviços
Requer várias regras	Regra única

Resposta direta à pergunta:

"Como eu habilito o DMZ e por que o DMZ é necessário?"

✔ **Habilitar o DMZ** significa configurar a ONT para enviar todo o tráfego externo para um único IP interno (que deve ser fixo).
✔ **O DMZ é necessário** quando o cliente precisa expor vários serviços, não sabe quais portas abrir ou quer validar rapidamente se o problema está no NAT.

Conclusão prática para suporte técnico

1. Verifique se o cliente tem **IP público**
2. Prefira **Port Forward** sempre que possível
3. Use **DMZ** apenas quando necessário
4. Nunca esqueça: **IP interno fixo**
5. Não decore ONTs → entenda o conceito