

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

Um resolver DNS aberto no seu VPS: porque é usado em ataques e como desligar a recursão

Segurança

CÓDIGO

RLX-MZ-KB-2254

VERSÃO

v2026.10.21

PAÍS · IDIOMA

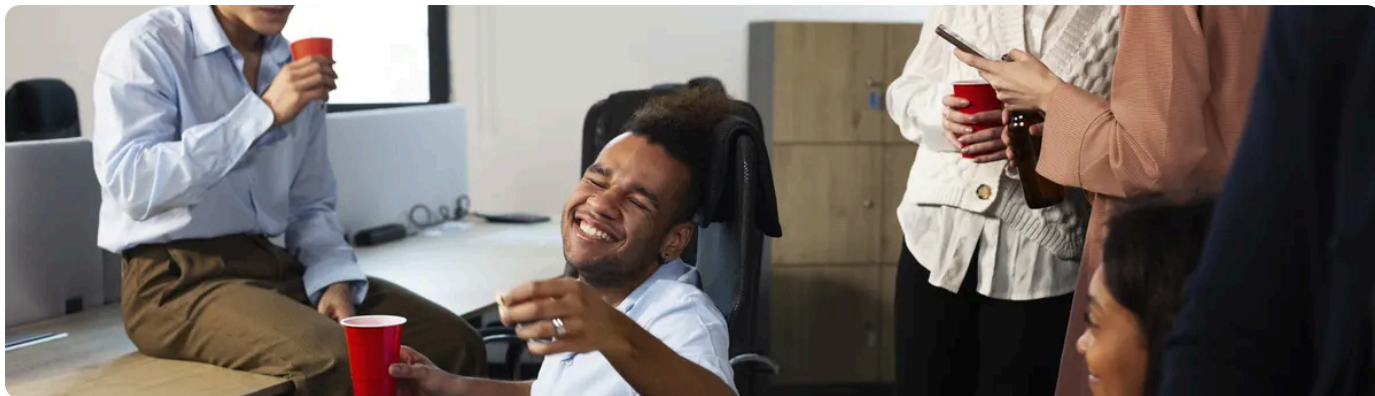
Moçambique · Português

Interweb Moçambique

RLX Holdings, S.A. · Grupo RLX Holdings

NUIT 401 191 607 · NUEL 105 045 974 · CAE 62022

<https://www.meu.interweb.co.mz/knowledgebase/2254>



Para quem tem um VPS ou um servidor dedicado com acesso root. A resposta curta: um resolver DNS aberto responde a perguntas sobre **qualquer** domínio vindas de **qualquer** endereço da internet, na porta **53**. Os atacantes mandam-lhe perguntas pequenas com o endereço de origem falsificado (o da vítima), e o seu servidor devolve à vítima respostas muito maiores: é um ataque de amplificação, e o seu VPS entra nele sem ter sido invadido. Uma equipa nacional de resposta a incidentes (CERT) encontra estes resolvers e o nosso fornecedor de rede envia-nos o aviso. Resolve-se desligando a **recursão** para fora, ou o serviço inteiro se não precisa dele, sem partir o DNS dos domínios que o servidor serve.

O que pode estar a responder na porta 53

O que corre	O que fazer
BIND (<code>named</code>), instalado por um painel ou à mão para ser o servidor de nomes dos seus domínios	Continua a responder pelos seus domínios, mas com a recursão desligada (ou só para o próprio servidor).
BIND ou Unbound instalados só para o servidor resolver nomes	Ponha-o a ouvir só em 127.0.0.1 e a recusar o resto.
dnsmasq, Pi-hole ou AdGuard Home num contentor com a porta 53 publicada	Retire a publicação para fora, ou limite na firewall aos endereços que o usam (por exemplo, os da sua VPN).
systemd-resolved em <code>127.0.0.53</code>	Não é um resolver aberto: só ouve no endereço local. Não precisa de mexer.
Um processo que não reconhece	Trate como suspeito: o meu VPS foi invadido?

Como fechar o resolver

1

Veja o que ouve na porta 53: `sudo ss -tulnp | grep ":53 "`

Endereços `0.0.0.0` , `:::` ou o IP público querem dizer que responde para fora.

2

Teste a partir de outra máquina: `dig @IP_DO_SERVIDOR`

`example.com` . Se vem uma resposta com endereço na secção ANSWER e a marca `ra` nas flags, o resolver está aberto. `status: REFUSED` ou tempo esgotado quer dizer fechado. Como ler a resposta: **dig e nslookup**.

3

Pergunte-se se precisa de DNS neste servidor. Veja para onde apontam os seus domínios com `dig NS asuaempresa.co.mz` . Se usam os servidores de nomes do registo ou de outro serviço, e não este VPS, pode desligar o serviço: `sudo systemctl disable --now named` (ou `bind9` , `unbound` , `dnsmasq` , conforme o que corre).

4

BIND que serve os seus domínios: dentro do bloco `options` que já existe (em Debian e Ubuntu, `/etc/bind/named.conf.options` ; na família Red Hat, `/etc/named.conf`), acrescente: `recursion no;`
`allow-query-cache { none; };` Se o próprio servidor usa o BIND para resolver nomes, em vez disso: `allow-recursion { 127.0.0.1; ::1; };`
`allow-query-cache { 127.0.0.1; ::1; };` Confirme e reinicie: `sudo named-checkconf`
`sudo systemctl restart named` (em versões antigas de Debian e Ubuntu o serviço chama-se `bind9`).

5

Unbound: na secção `server:` do `unbound.conf` : `interface:`
`127.0.0.1`
`access-control: 0.0.0.0/0 refuse`
`access-control: 127.0.0.0/8 allow` Depois `sudo unbound-`
`checkconf`
`sudo systemctl restart unbound`

6

dnsmasq ou um contentor: no `dnsmasq`, `listen-address=127.0.0.1`
e `bind-interfaces` . Num contentor, troque `"53:53/udp"` por
`"127.0.0.1:53:53/udp"` (e o mesmo para `tcp`), ou retire a publicação, e
`docker compose up -d` . Lembre-se de que a `ufw` não trava portas
publicadas pelo Docker: **Docker num VPS em segurança.**

7

Repita o teste do passo 2 de fora e guarde o resultado para o relatório.

8

Responda ao pedido de suporte no Meu Interweb, dentro do prazo do
aviso (curto, muitas vezes de um dia), com um relatório curto: a causa, o
que mudou e como confirmou que a porta já não responde de fora. Há um
modelo em **responder a um aviso de abuso**. Sem resposta, ou se o
problema continuar, o servidor pode ser desligado para proteger a rede,
com os dados intactos: **porque o servidor é desligado e como o
voltar a ligar.**

**Não feche a porta 53 nem pare o BIND num servidor que é o servidor de
nomes dos seus domínios:** os sites e o e-mail desses domínios deixam de ser
encontrados. Num servidor de nomes, a 53 fica aberta (UDP e TCP) e o que se fecha
é a recursão. Faça uma cópia dos ficheiros de configuração antes de os editar.

Este aviso não quer dizer que o servidor foi invadido: um resolver aberto é usado de fora, tal como está. Mesmo assim, responder ao aviso é obrigatório, e o tráfego de ataque pára quando a recursão fecha. Num VPS o acesso root é seu: nós não entramos no servidor nem mudamos a firewall que está lá dentro. Se ficar sem SSH, diga-nos no pedido de suporte.

Não sabe se o seu VPS é servidor de nomes dos seus domínios? Diga-nos no pedido de suporte quais são os domínios e o resultado do passo 1.

[Abrir pedido de suporte](#)

VEJA TAMBÉM

Um aviso de abuso sobre o seu servidor: o que significa, o prazo e o que precisamos de si

Responder a um aviso de abuso: a causa, o que removeu e como não se vai repetir

Verificar o DNS pela linha de comandos: dig e nslookup, e como ler a resposta

Configurar a firewall ufw no Ubuntu sem ficar de fora do servidor

Usar o Docker num VPS em segurança: as precauções que importam

Um ataque DDoS a partir do seu servidor: encontrar o tráfego de saída e pará-lo



Versão online deste documento

A Interweb é uma empresa líder em serviços de internet, com a missão de ajudar negócios a nascerem e prosperarem por meio da tecnologia.

2020

FUNDADA

37 mil+

CLIENTES

130+

INSCRIÇÕES POR DIA

Interweb Moçambique

RLX Holdings, S.A. • Grupo RLX Holdings

NUIT 401 191 607

NUEL 105 045 974

CAE 62022

SEDE Bairro 7 de Setembro
Vilankulo 1304 • CEP 0411-02, Inhambane, Moçambique

CONTACTOS info@interweb.co.mz • +258 84 635 1111 • +258 86 635 1111 • www.interweb.co.mz

HORÁRIO 2ª. à 6ª. Feira - 08 à 16 Horas
Sábado & Domingo - Fechado