

Brasil Distrito Federal Mundo Esportes
Metrópoles



ETRÓPOLES

Entretenimento Celebidades Últimas notícias

[Logar ou Criar uma Conta](#)

Fóruns

Site do Hardware

DNS para rede



Relacionados

Mais resultados? Use nossa pesquisa

1. Como liberar portas do modem p/ CFTV alguém endende?
2. Liberar um ip através do postfix

3. DNS
4. Problema com windows 98
5. Squid e Rotas

dns liberar



slackdi Junho 25, 2004

O que acontece é o seguinte, eu não consigo liberar os DNS para rede, eu tenho um servidor de DNS no ip 192.168.0.1, quando ele não consegue resolver os nomes ele manda para 200.189.80.2 e 200.189.80.10.

Quando eu rodo o firewall e vou em alguma estação e tento pingar por exemplo

ping pop.mail.yahoo.com.br

Não pinga, mas sem o firewall pinga, eu não consigo liberar o DNS, vou postar meu firewall.

```
#!/bin/sh
```

```
## Firewall ##
```

```
# Fazendo o flushing no Firewall
```

```
/usr/sbin/iptables -F
```

```
/usr/sbin/iptables -Z
```

```
/usr/sbin/iptables -X
/usr/sbin/iptables -t nat -F
/usr/sbin/iptables -P INPUT DROP
/usr/sbin/iptables -P FORWARD DROP
/usr/sbin/iptables -P OUTPUT ACCEPT

# Habilitando o roteamento e demais coisas

echo "1" > /proc/sys/net/ipv4/ip_forward
echo "1" > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts

# Liberando o ping para minha rede

/usr/sbin/iptables -A INPUT -s 192.168.0.0/24 -p icmp --icmp-type echo-request -m limit --limit 1/s -j
ACCEPT

# Contra pacotes nao estabilizados

/usr/sbin/iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

# Nao aceita pacotes fragmentados

/usr/sbin/iptables -A INPUT -i ppp0 -f -j DROP
/usr/sbin/iptables -A INPUT -i ppp0 -s 192.168.0.0/24 -j DROP

# Liberando o acesso ao Squid e Jabber para minha rede

/usr/sbin/iptables -A INPUT -p TCP -i eth0 -s 192.168.0.0/24 --dport 3128 -j ACCEPT
/usr/sbin/iptables -A INPUT -p TCP -i eth0 -s 192.168.0.0/24 --dport 5222 -j ACCEPT

# Liberando o acesso ao SSH e FTP

/usr/sbin/iptables -A INPUT -p TCP --dport 8888 -j ACCEPT
/usr/sbin/iptables -A INPUT -p TCP --dport 6666 -j ACCEPT

# Libera o acesso de servidores www para meu squid

/usr/sbin/iptables -A INPUT -p TCP -i ppp0 --sport 80 -j ACCEPT
/usr/sbin/iptables -A INPUT -p TCP -i ppp0 --sport 443 -j ACCEPT
/usr/sbin/iptables -A INPUT -p TCP -i ppp0 --sport 20 -j ACCEPT
/usr/sbin/iptables -A INPUT -p TCP -i ppp0 --sport 21 -j ACCEPT

# Libera o DNS para rede

/usr/sbin/iptables -A INPUT -p udp -s 192.168.0.0/24 -d 200.189.80.2 --dport 53 -j ACCEPT
/usr/sbin/iptables -A INPUT -p udp -s 192.168.0.0/24 -d 200.189.80.10 --dport 53 -j ACCEPT
```

```
/usr/sbin/iptables -A INPUT -p udp -s 200.189.80.2 --sport 53 -d 192.168.0.0/24 -j ACCEPT
/usr/sbin/iptables -A INPUT -p udp -s 200.189.80.10 --sport 53 -d 192.168.0.0/24 -j ACCEPT

# Barra porcarias do FORWARD

/usr/sbin/iptables -A FORWARD -m state --state INVALID -j DROP

# Aceita conexoes estabilizadas

/usr/sbin/iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT

# Liberando respostas dos DNS para rede

/usr/sbin/iptables -A FORWARD -p udp -s 192.168.0.0/24 -d 200.189.80.2 --dport 53 -j ACCEPT
/usr/sbin/iptables -A FORWARD -p udp -s 192.168.0.0/24 -d 200.189.80.10 --dport 53 -j ACCEPT
/usr/sbin/iptables -A FORWARD -p udp -s 200.189.80.2 --sport 53 -d 192.168.0.0/24 -j ACCEPT
/usr/sbin/iptables -A FORWARD -p udp -s 200.189.80.10 --sport 53 -d 192.168.0.0/24 -j ACCEPT

# Libera as portas do Outlook para a rede

/usr/sbin/iptables -A FORWARD -p TCP -s 192.168.0.0/24 --dport 25 -j ACCEPT
/usr/sbin/iptables -A FORWARD -p TCP -s 192.168.0.0/24 --dport 110 -j ACCEPT
/usr/sbin/iptables -A FORWARD -p tcp --sport 25 -j ACCEPT
/usr/sbin/iptables -A FORWARD -p tcp --sport 110 -j ACCEPT

# Nega qualquer redirecionamento de portas

/usr/sbin/iptables -t nat -A PREROUTING -j DROP

# Regra para que todas as maquinas passem pelo proxy

/usr/sbin/iptables -t nat -A PREROUTING -s 192.168.0.0/24 -p tcp --dport 80 -j DROP

# Mascara a conexao

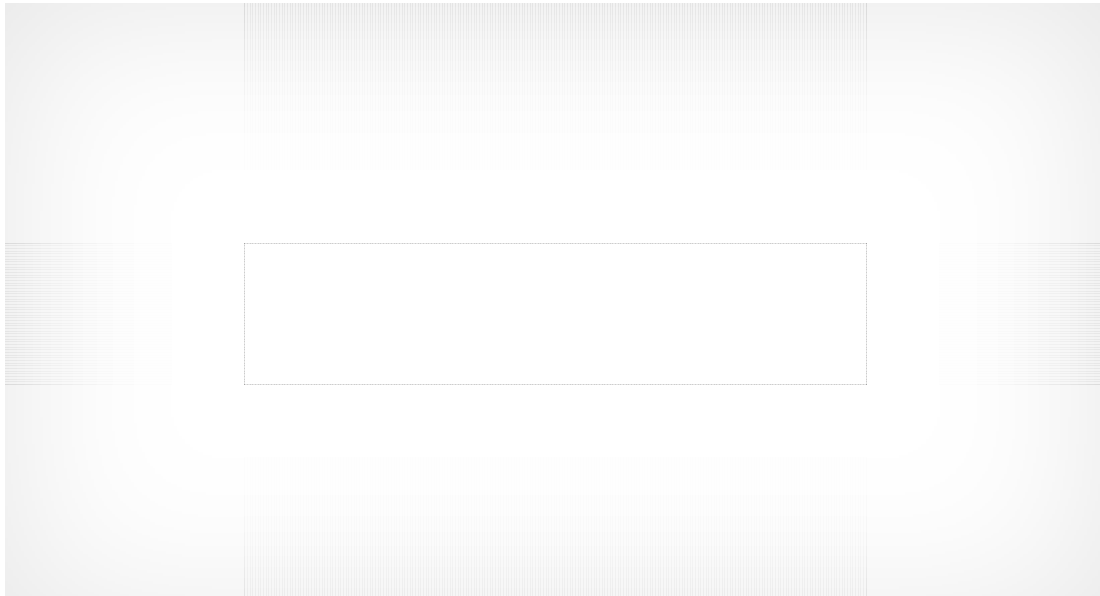
/usr/sbin/iptables -t nat -A POSTROUTING -j MASQUERADE

echo "Conexao a Internet protegida, firewall ativado"

-----

Galera HELP ..
```

PUBLICIDADE



jqueiroz Junho 25, 2004

Libera o DNS para rede

```
/usr/sbin/iptables -A INPUT -p udp -s 192.168.0.0/24 -d 200.189.80.2 --dport 53 -j ACCEPT
/usr/sbin/iptables -A INPUT -p udp -s 192.168.0.0/24 -d 200.189.80.10 --dport 53 -j ACCEPT
/usr/sbin/iptables -A INPUT -p udp -s 200.189.80.2 --sport 53 -d 192.168.0.0/24 -j ACCEPT
/usr/sbin/iptables -A INPUT -p udp -s 200.189.80.10 --sport 53 -d 192.168.0.0/24 -j ACCEPT
(...)
```

Liberando respostas dos DNS para rede

```
/usr/sbin/iptables -A FORWARD -p udp -s 192.168.0.0/24 -d 200.189.80.2 --dport 53 -j ACCEPT
/usr/sbin/iptables -A FORWARD -p udp -s 192.168.0.0/24 -d 200.189.80.10 --dport 53 -j ACCEPT
/usr/sbin/iptables -A FORWARD -p udp -s 200.189.80.2 --sport 53 -d 192.168.0.0/24 -j ACCEPT
/usr/sbin/iptables -A FORWARD -p udp -s 200.189.80.10 --sport 53 -d 192.168.0.0/24 -j ACCEPT
```

Acho que vc está sendo muito restritivo com o DNS. Simplesmente libere-o...

```
iptables -A FORWARD -p udp -s 192.168.0.0/24 --dport 53 -j ACCEPT
```

e chega: o reverso já é aceito na regra "--state STABLISHED,RELATED". Aliás, reveja seu script; quando vc usa essa regra, não é necessário criar regras pra liberar o tráfego reverso.

Outra coisa: as regras que vc pôs liberando DNS pra cadeia INPUT são inúteis. Se vc tem um servidor DNS nessa máquina, a regra deve ser:

```
iptables -A INPUT -p udp -s 192.168.0.0/24 --dport 53 -j ACCEPT
```

sem endereço de destino; se a cadeia é INPUT, o endereço de destino tem que ser o IP do firewall, ou 127.0.0.1 (localhost).

outra coisa: as regras do iptables são processadas em sequência; então vc tem que começar com as regras

mais específicas, pra depois colocar as mais gerais. então o trecho...

```
# Nega qualquer redirecionamento de portas

#/usr/sbin/iptables -t nat -A PREROUTING -j DROP

# Regra para que todas as maquinas passem pelo proxy

/usr/sbin/iptables -t nat -A PREROUTING -s 192.168.0.0/24 -p tcp --dport 80 -j DROP
```

... pode não funcionar direito, pois ele primeiro vai negar tudo, pra depois negar (?) um caso específico (???).



M81xb Junho 25, 2004

Poiseh, voce configurou seu servidor de DNS para perguntar aos outros servidores DNS o que ele nao sabe, nao eh? Entao o unico servidor de DNS que os CLIENTES precisam consultar eh o SEU servidor de DNS.

O resto funciona neh? Se voce pingar IPs da net, eles funcionam corretamente, certo?

EDIT: A funcao dessa mensagem eh ver se voce tem certeza que seu servidor DNS esta configurado para perguntar aos outros servidores DNS sobre IPs que ele nao conhece e ver se o firewall esta funcionando corretamente, alem do fato de estar bloqueando o servidor de DNS.



slackdi Junho 26, 2004

Bom jqueiroz eu não manjo nada de firewall to começando a aprender, vou testar na segunda-feira isso que você disse.

fernando, eu configurei meu servidor de DNS para perguntar aos outros quando ele não consegue resolver, sem o firewall tudo funciona, mas com o firewall não funciona.

Valeu pessoal pela ajuda vou testar e posto o resultado.



slackdi Junho 28, 2004

Eu comentei todas essas regras:


Liberando respostas dos DNS para rede

```
/usr/sbin/iptables -A FORWARD -p udp -s 192.168.0.0/24 -d 200.189.80.2 --dport 53 -j ACCEPT
/usr/sbin/iptables -A FORWARD -p udp -s 192.168.0.0/24 -d 200.189.80.10 --dport 53 -j ACCEPT
/usr/sbin/iptables -A FORWARD -p udp -s 200.189.80.2 --sport 53 -d 192.168.0.0/24 -j ACCEPT
/usr/sbin/iptables -A FORWARD -p udp -s 200.189.80.10 --sport 53 -d 192.168.0.0/24 -j ACCEPT
```

E coloquei no lugar essa

```
iptables -A FORWARD -p udp -s 192.168.0.0/24 --dport 53 -j ACCEPT
```


Mas mesmo assim ai não funcionou.

 **jqueiroz** Junho 28, 2004

Vai no firewall/servidor DNS, e use:

```
host www.forumgdh.net
```


e veja se lá o DNS está funcionando 100%.

 **slackdi** Junho 28, 2004

Não entendi o teste, acho que era para digitar esse comando no servidor correto ?

Uma coisa meu servidor de DNS ta blz .. já tetssei varias vezes ..


Só o iptables que não libera mesmo

 **jqueiroz** Junho 28, 2004

tem como vc fazer um dump dos pacotes? Se vc tiver o tcpdump instalado, pode fazer:

```
tcpdump -vvv ip and udp and port 53
```

em seguida, tentar alguma consulta de DNS nos clientes, pra ver se os pacotes chegam ou não.

 **slackdi** Junho 28, 2004

Eu tenho o tcpdump instalado, mas não consegui dar esse comando da sintaxe error.

Mas eu tenho certeza que meu servidor de DNS está funcionando, pois sem ele as estações não conseguem resolver os IPs

 **jqueiroz** Junho 28, 2004


Putz... há quanto tempo estamos olhando pra essa coisa, e não percebemos?

```
# Nao aceita pacotes fragmentados
```

```
/usr/sbin/iptables -A INPUT -i ppp0 -f -j DROP
```

```
/usr/sbin/iptables -A INPUT -i ppp0 -s 192.168.0.0/24 -j DROP
```

Cadê o "-f" da segunda linha? Ele não está barrando os pacotes fragmentados... está barrando tudo...

 **slackdi** Junho 28, 2004

cara eu fui numa estação com o firewall desabilitado e dei um tracert olha o resultado.

Rastreando a rota para pop.vip.sc5.yahoo.com [216.136.173.10]

com no máximo 30 saltos:

1 16 ms <10 ms <10 ms 192.168.0.254

2 31 ms 47 ms 47 ms cnet-cable-189-84-1.canbrasnet.com.br [200.189.84.1]

3 31 ms 47 ms 47 ms router.canbrasnet.com.br [200.189.80.1]

4 63 ms 62 ms 47 ms embratel-A4-0-50-dist04.spo.embratel.net.br [200.228.240.137]

5 47 ms 62 ms 63 ms ebt-G5-0-core03.spo.embratel.net.br [200.230.219.208]

6 47 ms 47 ms 47 ms ebt-P6-0-intl01.spo.embratel.net.br [200.230.1.153]

7 141 ms 156 ms 172 ms ebt-so-0-0-1-intl01.mia6.embratel.net.br [200.230.3.26]

8 * * * Esgotado o tempo limite do pedido.

9 156 ms 172 ms 187 ms 0.so-1-1-0.XR1.MIA4.ALTER.NET [152.63.85.2]

10 297 ms 235 ms 312 ms 0.so-4-2-0.XL1.MIA4.ALTER.NET [152.63.101.42]

11 797 ms 828 ms 782 ms 0.so-4-0-0.XL1.ATL5.ALTER.NET [152.63.86.190]

12 703 ms 703 ms 734 ms 0.so-7-0-0.XR1.ATL5.ALTER.NET [152.63.85.190]

13 * 687 ms 703 ms 193.ATM6-0.BR1.ATL5.ALTER.NET [152.63.80.113]

14 203 ms 219 ms 188 ms 204.255.168.74

15 625 ms 687 ms 672 ms agr4-loopback.Atlanta.savvis.net [208.172.66.104]

16 719 ms 703 ms 718 ms dcr2-as0-0.Atlanta.savvis.net [208.172.67.53]

17 250 ms 219 ms 265 ms dcr2-loopback.SanFranciscosfo.savvis.net [206.24.210.100]

18 250 ms 234 ms 266 ms bhr1-pos-13-0.SantaClarasc4.savvis.net [208.172.147.106]

19 235 ms 265 ms 235 ms csr3-ve241.SantaClarasc5.savvis.net [64.56.192.138]

20 250 ms 297 ms 250 ms g2-1.bas1-m.sc5.yahoo.com [64.56.207.146]

21 250 ms 266 ms 250 ms vl41.bas1-m.sc5.yahoo.com [66.163.160.202]

22 266 ms 265 ms 235 ms pop.vip.sc5.yahoo.com [216.136.173.10]

Rastreamento completo.



slackdi Junho 29, 2004

Você tem uma rede windows com um servidor de DNS e Arquivos no ip 192.168.0.1 que quando não consegue resolver nome pede ajuda para 200.189.80.2 e 200.189.80.10. Agora você tem um firewall linux que compartilha a net (ppp0) para as outras máquinas através do squid. Que regras de firewall você usaria para fechar tudo e conseguir na estação dar um ping login.icq.com e o servidor de DNS conseguir resolver esse nome para você ?



jqueiroz Junho 29, 2004

slack, vc verificou aquela linha que eu falei? A que deveria estar bloqueando pacotes fragmentados?

Em tempo: fragmentação faz parte do jogo; não acho que os ataques que tentam se aproveitar de fragmentação sejam motivo suficiente para bloquear todos os pacotes fragmentados.



slackdi Junho 29, 2004

Sim, meu firewall ta zerado .. só está com as linhas que fazer o forward .. mas nada .. mas mesmo assim não libera ..

quer começar um firewall para liberar e depois fecho as coisa .. mas ta soda



M81xb Junho 29, 2004

Quais as linhas que tem agora? Deve ser algo que voce esqueceu de adicionar para permitir a passagem dos pacotes, porque aposto que se voce tirar os "-P DROP" ele funciona



jqueiroz Junho 29, 2004

aposto que se voce tirar os "-P DROP" ele funciona

se tirar os "-P DROP" é melhor tirar o fwl todo :lol:



M81xb Junho 29, 2004

jqueiroz disse:

aposto que se voce tirar os "-P DROP" ele funciona

se tirar os "-P DROP" é melhor tirar o fwl t...

Mas nao precisaria de pelo menos as regra que fazem o roteamento(NAT)? Dai nao pode tirar **todo** o firewall Fora isso voce esta certo hehe



slackdi Junho 29, 2004

Galera, continuando meus testes observei que mesmo para o firewall ele não consegue pingar na net.

Como eu defini a politica padrão de INPUT para DROP, eu não liberei nada na interface de internet (ppp0)

Como eu posso estar liberando meu firewall para navegar na net ?

Acho que esse é o caminho para liberar o DNS para rede.

Vamos lá galera ajuda ai ...



M81xb Junho 29, 2004

slackdi disse:

Galera, continuando meus testes observei que mesmo para o firewall ele não consegue pingar na net.

Como eu defini ...

Isso me parece mais problema de output... mantenha seu script como esta, mas ponha um linha temporaria no final: /sbin/iptables -P OUTPUT ACCEPT, so para ter certeza que nao eh problema de output.

Alias cara, desculpa dar as resposta pedaco por pedaco (ao inves de uma solucao definitiva), mas que eu nao saco muito de iptables, to tentando minimizar o terreno para encontrar o problema Mas quem sabe o **jqueiroz** ou algum outro colega do forum possa te dar uma solucao definitiva.



slackdi Junho 30, 2004

fernandoAzambuja, obrigado pela ajuda cara sou muito grato.

coloquei essa linha no final mas continua a mesma coisa o diaxo ...



