ZuNET
PROVEDOR DE INTERNET

GUIA COMPLETO

Controle de P2P

Compatilhadores de arquivos

CONTROLE DE P2P

CONTROLE GERAL DE CONEXÕES PARA SOFTWARES COMPARTILHADORES DE ARQUIVOS.

Sabemos que os softwares de compartilhamento de arquivos, como emule, kazaa, torrent e outros são como uma praga consumir banda do link dos provedores. Eles fazem muitas conexões e praticamente ocupam toda a banda destinada ao cliente. Na maioria das vezes deixando a navegação e outros serviços do cliente lento demais. O que acaba por compromoter a qualidade dos serviços dos provedores ou a produtividade das empresas.

Apresentamos como solução um controle dessas “pragas” visando resolver problemas desse tipo em horários críticos de uso do link. Utilizamos nesta solução o FIREWALL, QUEUES, SCRIPTS e SCHEDULER. Do MIKROTIK.

No quadro abaixo (em azul), esta o que preciso de forma completa para obter sucesso nesse controle. Para executar o script abaixo é preciso apenar copiar (CRTL+C) todo o texto delimitado no referido quadro e colocar no NEW TERMINAL do mikrotik se estiver usando WINBOX, ou no console do SSH ou TELNET conforme seja a preferência do administrador do servidor.

Qualuer contribuição será bem vinda através do e-mail: suporte@redezunet.com.br

```
/ ip firewall mangle
add chain=prerouting p2p=all-p2p action=mark-connection new-connection-
mark=conexao-p2p passthrough=yes comment="CONTROLE DO P2P" disabled=no
add chain=prerouting connection-mark=conexao-p2p action=mark-packet new-packet-
mark=pacotes-p2p passthrough=yes comment="" disabled=no
add chain=prerouting p2p=all-p2p action=mark-routing new-routing-mark=p2p
passthrough=no comment="" disabled=no
/ip firewall filter
add chain=forward p2p=all-p2p src-address-list=!p2p-sem-bloqueio action=drop
comment="BLOQUEIO DO P2P" disabled=yes
/ queue tree
add name="\[P2P\] - Download" parent=global-in packet-mark=pacotes-p2p limit-at=0
queue=default priority=8 max-limit=64000 burst-limit=0 burst-threshold=0 burst-
time=0s disabled=no
add name="\[P2P\] - Upload" parent=global-out packet-mark=pacotes-p2p limit-at=0
queue=default priority=8 max-limit=64000 burst-limit=0 burst-threshold=0 burst-
time=0s disabled=no
/ system script
add name="liberar-p2p" source="/ip firewall filter disable \[/ip firewall filter
find p2p=all-p2p\]" \ policy=ftp,reboot,read,write,policy,test,winbox
add name="bloquear-p2p" source="/ip firewall filter enable \[/ip firewall filter
find p2p=all-p2p\]" \ policy=ftp,reboot,read,write,policy,test,winbox
/ system scheduler
add name="bloquear-p2p" on-event=bloquear-p2p start-date=aug/31/2007 start-
time=08:00:00 interval=1d comment=""  disabled=no
add name="liberar-p2p" on-event=liberar-p2p start-date=aug/31/2007 start-
time=21:00:00 interval=1d comment="" disabled=no
```

DETALHAMENTO E EXPLICAÇÕES PERTINENTES

FIREWALL

O primeiro passo para construirmos nosso CONTROLE DE P2P é exatamente marcando os pacotes e as conexões e até mesmo a rota desses pacotes para uso no futuro em outras aplicação como por exemplo o SUPER LOAD BALANCED que desenvolvemos com sistema misto de balancemento de link.

Marcaremos as conexões do p2p e daremos um nome a ela "conexao-p2p", ainda comentaremos essa regra no intuito de identificar todo o conjunto do mangle utilizado nesse controle.

```
/ip firewall mangle
add chain=prerouting p2p=all-p2p action=mark-connection new-connection-
mark=conexao-p2p passthrough=yes comment="CONTROLE DO P2P" disabled=no
```

Já marcamos as conexões agora precisaremos marcar os pacotes que trafegam nas conexões marcadas acima, afim de podermos tratá-los posteriormente.

```
/ip firewall mangle
add chain=prerouting connection-mark=conexao-p2p action=mark-packet new-
packet-mark=pacotes-p2p passthrough=yes comment="" disabled=no
```

Em alguns casos, quando for preciso definir alguma rota específica para as conexões e os pacotes tratados acima, principalmente quando trabalhamos com mais de um link, e quisermos definir por qual link exatamente sairá o tráfego p2p de nossa rede, devemos incluir a regra abaixo. Mas lembre-se que ela só se aplica em casos de LOAD BALANCED.

```
/ip firewall mangle
add chain=prerouting p2p=all-p2p action=mark-routing new-routing-mark=p2p
passthrough=no comment="" disabled=no
```

Também incluíremos uma regra no firewall que vai bloquear todo tráfego de p2p, mas por padrão ela será inserida em nosso servidor em modo desabilitado. Esta regra será manipulada por dois scripts descritos mais adiante, que habilitarão e dasabilitarão esta regra atraves de um agendamento.

```
/ip firewall filter
add chain=forward p2p=all-p2p src-address-list=!p2p-sem-bloqueio
action=drop comment="BLOQUEIO DO P2P" disabled=yes
```

Pronto!! Tudo o que precisavamos fazer no firewall já fizemos, agora precisaremos fazer o controle de banda do p2p, apara previnir um consumo excessivo de link apenas por estas "pragas".

Passemos então para o Queues Tree que vai controlar a banda geral das conexões e pacotes que marcamos no Mangle.

QUEUES

Bom depois de termos tudo que queremos identificado pelo mangle vamos agora etipular duas outras regras de controle de banda, para ajudar todo o tráfego p2p em nossa rede a uma determinada banda. Lembrando que estamos nos referindo apenas ao consumo geral do p2p, preservando a banda de cada cliente.

Primeiro vamos controlar os downloads do p2p em "***max-limit=64000***" ou seja 64k, mas este valor deve ser ajustado a conveniência e necessidade de cada um.

```
/ queue tree
add name="\[P2P\] - Download" parent=global-in packet-mark=pacotes-p2p
limit-at=0 queue=default priority=8 max-limit=64000 burst-limit=0 burst-
threshold=0 burst-time=0s disabled=no
```

Agora que controlamos a entrada (download), vamos fazer o mesmo com a saída (upload) também com "***max-limit=64000***" ou seja 64k.

```
/ queue tree
add name="\[P2P\] - Upload" parent=global-out packet-mark=pacotes-p2p
limit-at=0 queue=default priority=8 max-limit=64000 burst-limit=0 burst-
threshold=0 burst-time=0s disabled=no
```

Pronto!!! O controle de banda para o p2p está ativo e isso siginifica que todos os clientes de sua rede estão submetidos a este controle.

SCRIPTS

Analisando bem o que fizemos até agora vamos concluir que limitamos o uso de banda para o p2p, mas muitas vezes mesmo limitando a banda que já é um avanço e um diferencial para o melhor gerencimaneto de nossa banda, ainda precisaremos em algum momento parar em momentos críticos de uso do link alguns serviços, como estamos tratando de p2p, e o dito cujo que iremos parar ou liberar dependendo do caso. Para isso vamos automatizar usando dois scripts simples esta tarefa, tirando as mãos do nosso firewall minimizando a chance de algo dar errado.

Este script desabilita se estiver habilitada, e libera o p2p aquela regrinha que mencionamos acima:

```
/ system script
add name="liberar-p2p" source="/ip firewall filter disable \[/ip firewall
filter find p2p=all-p2p\]" \
policy=ftp,reboot,read,write,policy,test,winbox
```

Este script habilita aquela regra e desabilita o tráfego do p2p:

```
/ system script
add name="bloquear-p2p" source="/ip firewall filter enable \[/ip firewall
filter find p2p=all-p2p\]" \
policy=ftp,reboot,read,write,policy,test,winbox
```

SCHEDULER

Uma vez criado o script de bloqueio e liberação do p2p, podemos agendá-lo para ser executado automaticamente. Bloqueando todos os dias às 8h e liberando às 21h, deixando esta banda, apesar de controlada pelo queue, livre para uso de outros serviços.

```
/ system scheduler
add name="bloquear-p2p" on-event=bloquear-p2p start-date=aug/31/2007
start-time=08:00:00 interval=1d comment="" disabled=no
add name="liberar-p2p" on-event=liberar-p2p start-date=aug/31/2007 start-
time=21:00:00 interval=1d comment="" disabled=no
```

Tudo pronto se chegamos até aqui é por que tudo deu certo e esse guia de controle de p2p esta funcionando com sucesso. Mas ainda não acabou. Fizemos regras precisamos tratar as exceções agora de modo a não deixar o nosso sistema quadradão.

PERGUNTAS FREQUENTES:

01) Como faço para não bloqueador o tráfego p2p de um determinado endereço de ip?

Quando este guia estava em análise e as regras sendo testadas em produção no nosso provedor, nos deparamos com esse problema de imediato, no entanto pesquisamos várias alternativas e dentre as quais melhor obtivemos resultado foi a de utilizar um adress-list para livrar do bloqueio do horário.

Solução 1 – Liberando apenas um ip do bloqueio:

```
/ ip firewall address-list
add list=p2p-sem-bloqueio address=xxx.xxx.xxx.xxx comment="" disabled=no
```

Onde "**xxx.xxx.xxx.xxx**" é o ip que deseja liberar, vc pode repetir para todo o ip que desejar liberar.

Solução 2 – Liberando para um rede inteira:

```
/ ip firewall address-list
add list=p2p-sem-bloqueio address=xxx.xxx.xxx.xxx/24 comment=""
disabled=no
```

Onde "**xxx.xxx.xxx.xxx/24**" é a rede para qual vc deseja liberar.