EXEMPLO DE

IMPLANTAÇÃO E CONFIGURAÇÃO NAS MODO ALL-PPPOE-MIKROTIK

Kiraz Log Forense

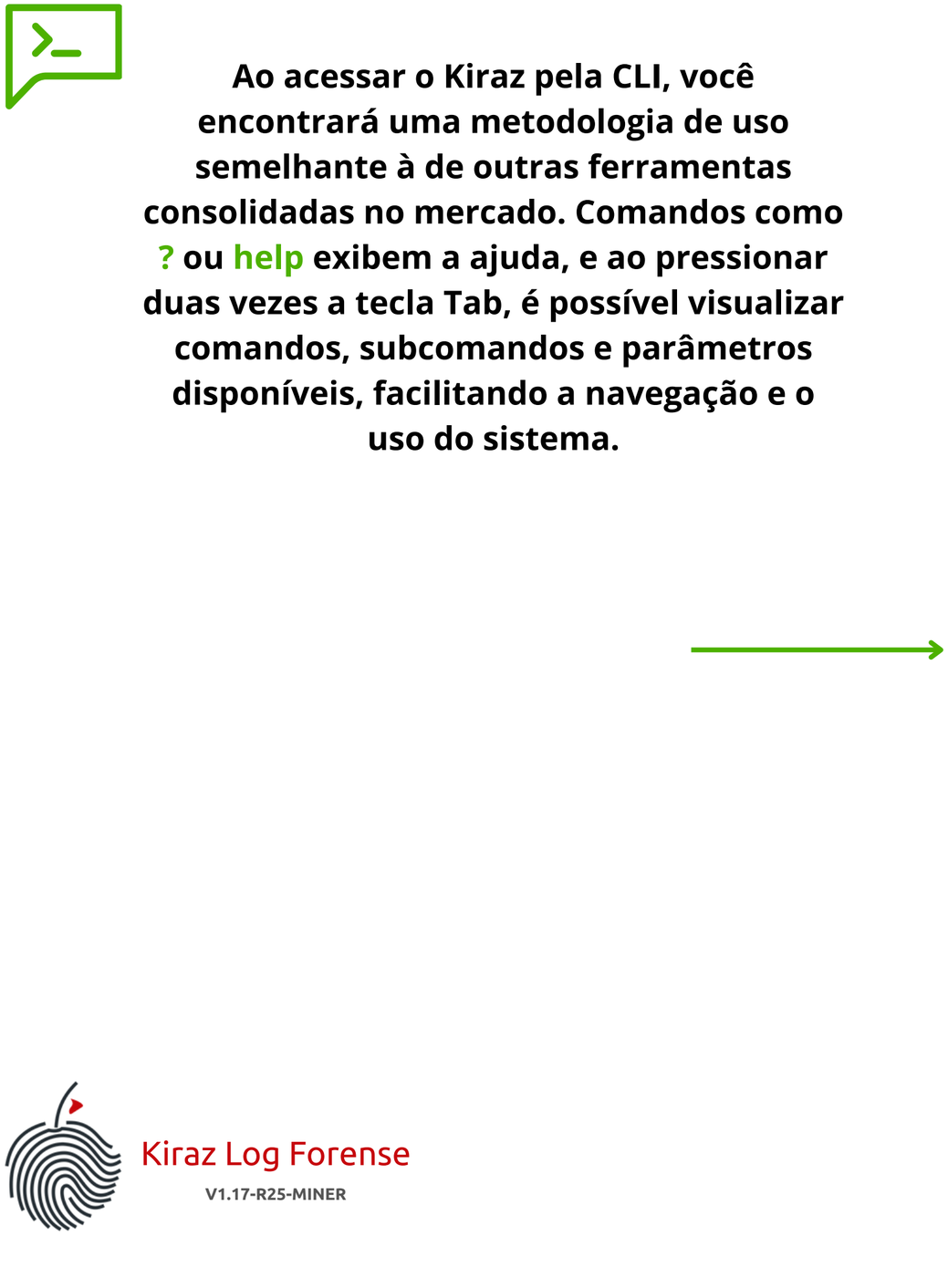
V1.17-R25-MINER

Topologia

all-pppoe-mikrotik

Após a instalação e ativação da licença do Kiraz, neste exemplo utilizaremos a aplicação no modo all-pppoe-mikrotik. Nesse modo, as regras de configuração devem ser aplicadas diretamente em cada concentrador (NAS). O sistema é capaz de capturar inclusive a interface de rede utilizada pelo cliente PPPoE, garantindo que essas informações sejam enviadas e armazenadas junto aos registros de log.

Ao acessar o Kiraz pela CLI, você encontrará uma metodologia de uso semelhante à de outras ferramentas consolidadas no mercado. Comandos como ? ou help exibem a ajuda, e ao pressionar duas vezes a tecla Tab, é possível visualizar comandos, subcomandos e parâmetros disponíveis, facilitando a navegação e o uso do sistema.



Topologia

all-pppoe-mikrotik

Kiraz Log Forense

V1.17-R25-MINER

Topologia

all-pppoe-mikrotik

Após o login, o comando vendors permite acessar a seção de fabricantes homologados. Em seguida, o comando list exibirá todos os vendors atualmente disponíveis. Essa lista é constantemente atualizada pela nossa equipe de homologação. Também disponibilizamos, tanto na instalação quanto em nosso site, o arquivo completo com os dispositivos homologados.

Neste exemplo, trabalharemos com o vendor 1 - Mikrotik_ALL-PPP, que representa a integração com concentradores Mikrotik utilizando o modo PPPoE completo.

```
[admin@KirazLogMiner] > ?

Comandos disponíveis:

  devices          - Gerenciamento de Dispositivos.
  format           - Formata discos adicionais para uso como armazenamento de logs.
  listlogpath      - Exibe o caminho de logs atualmente configurado.
  logout           - Faz logout do usuário atual e retorna para a tela de autenticação.
  logpath          - Exibe todos os discos disponíveis para seleção.
  logsforenses     - Gerenciamento de Logs Forenses.
  reboot           - Reinicia o sistema.
  setlogpath       - Define um novo caminho de logs para armazenamento.
  setpassword      - Altera a senha do usuário atual.
  show             - Exibe informações conforme o parâmetro informado.
  shutdown         - Desliga o sistema.
  start            - Inicia a mineração de logs (escuta e grava) ou apenas escuta (listen).
  stop             - Para o processo de mineração ou escuta.
  users            - Gerenciamento de Usuários.
  vendors          - Gerenciamento de Vendors (diferentes fabricantes).
  version          - Exibe a versão atual do sistema.

[admin@KirazLogMiner] > vendors
[admin@KirazLogMiner] (vendors) > list
Lista de Vendors (Modo Simplificado):
ID    | Name
----------------------------
1       Mikrotik_ALL-PPP
2       Mikrotik_CGN
[admin@KirazLogMiner] (vendors) >
```

Topologia

all-pppoe-mikrotik

Agora, utilize o comando exit para sair da seção de vendors. Em seguida, use o comando devices para acessar a seção de dispositivos, onde serão cadastrados os concentradores (NAS) utilizados para autenticação PPPoE.

```
[admin@KirazLogMiner] (vendors) > list
Lista de Vendors (Modo Simplificado):
ID    | Name
---------------------------
1       Mikrotik_ALL-PPP
2       Mikrotik_CGN
[admin@KirazLogMiner] (vendors) > exit
[admin@KirazLogMiner] >
[admin@KirazLogMiner] > devices
[admin@KirazLogMiner] (devices) > ?

Comandos disponíveis:

  add             - Adiciona um device.
  delete          - Deleta um device.
  disable_all     - Desabilita todos os devices cadastrados.
  edit            - Edita um device.
  enable_all      - Habilita todos os devices cadastrados.
  exit            - Sai do modo devices.
  list            - Lista todos os devices cadastrados.

[admin@KirazLogMiner] (devices) >
add          delete       disable_all  edit         enable_all   exit         help         list
[admin@KirazLogMiner] (devices) > list
Nenhum device cadastrado.
[admin@KirazLogMiner] (devices) >
```

Topologia

all-pppoe-mikrotik

Você pode cadastrar cada NAS individualmente, especificando todos os dados e diferenciando as portas de coleta conforme necessário.
No entanto, no exemplo ao lado, faremos um cadastro do tipo “geral”, aplicável a todos os concentradores, utilizando a porta padrão 514.
Os parâmetros mínimos exigidos para o cadastro são: nome do dispositivo, porta e o ID do vendor, conforme ilustrado na figura ao lado.

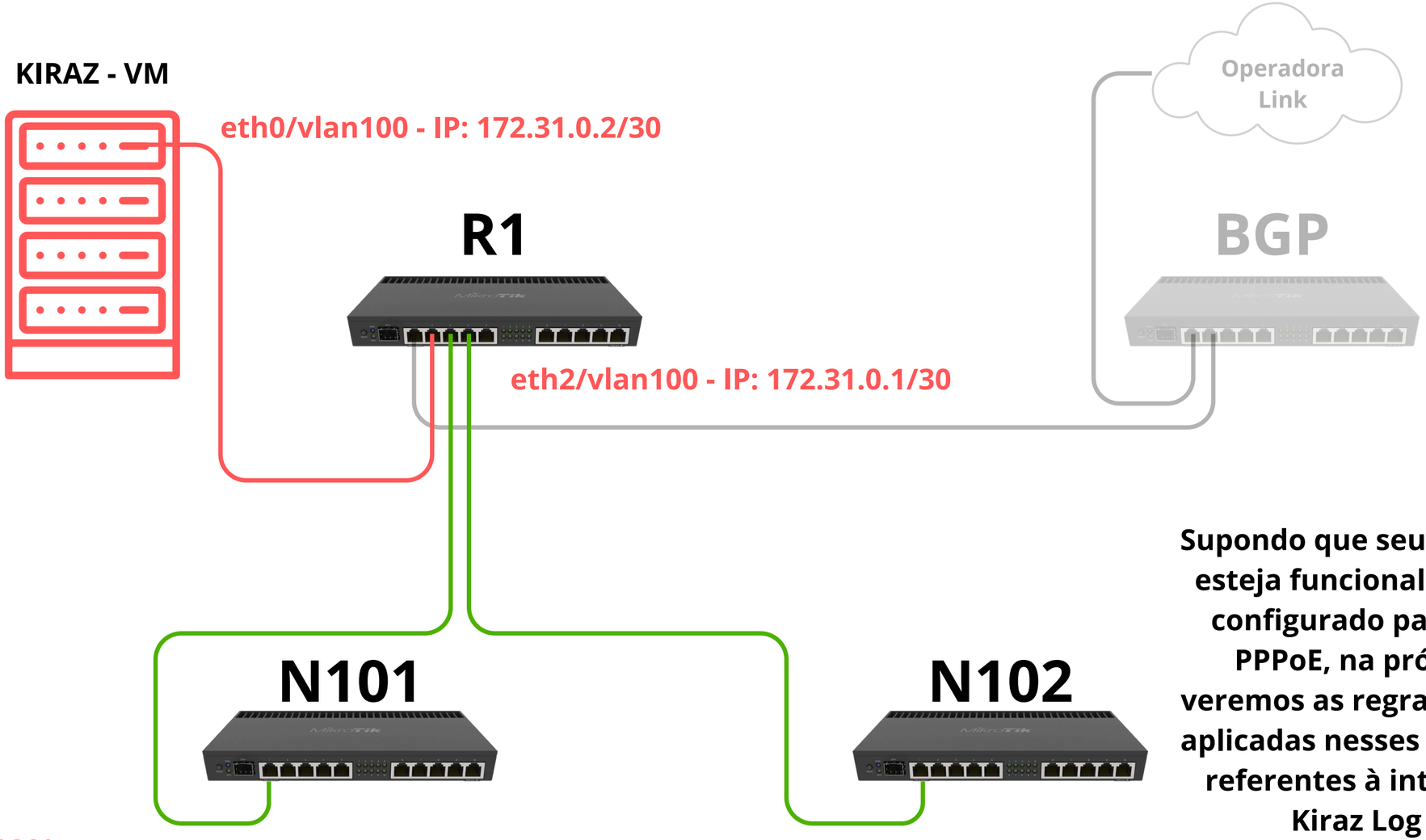
```
[admin@KirazLogMiner] (devices) >
add          delete       disable_all  edit         enable_all   exit         help         list
[admin@KirazLogMiner] (devices) > list
Nenhum device cadastrado.
[admin@KirazLogMiner] (devices) > add
description=  device_name=  enabled=      ip_address=   password=     port=         protocol=     remote_port=  user=         vendor_id=
[admin@KirazLogMiner] (devices) > add
Parâmetros obrigatórios: device_name, port e vendor_id.
[admin@KirazLogMiner] (devices) >
[admin@KirazLogMiner] (devices) > add device_name=todos port=514 vendor_id=1
Device 'todos' adicionado com sucesso.
[admin@KirazLogMiner] (devices) > list
Lista de Devices (Modo Simplificado):
ID       | Name                 | Protocol   | Port   | IP Address         | Enabled   | Vendor
-------------------------------------------------------------------------------------------------------
1          todos                  UDP          514      -                    Yes         1 (Mikrotik_ALL-PPP)
[admin@KirazLogMiner] (devices) > list verbose
Lista de Devices (Modo Verbose):

ID:          1
Name:        todos
Protocol:    UDP
Port:        514
IP Address:  -
User:        -
Password:    -
RemotePort:  -
VendorID:    1 (Mikrotik_ALL-PPP)
Enabled:     Yes
Description: -
---------------------------------------
[admin@KirazLogMiner] (devices) >
```

Agora vamos aplicar as regras e configurações nos concentradores. Abaixo, apresentamos uma topologia de exemplo com dois NAS para ilustrar o cenário.

Topologia

all-pppoe-mikrotik



Supondo que seu concentrador já esteja funcional e devidamente configurado para operar com PPPoE, na próxima página veremos as regras que devem ser aplicadas nesses concentradores, referentes à integração com o Kiraz Log Forense.

/system logging action
add name=KirazLogForense remote=172.31.0.2 target=remote

/system logging
set 0 topics=info,!firewall
add action=KirazLogForense prefix=N101 topics=firewall

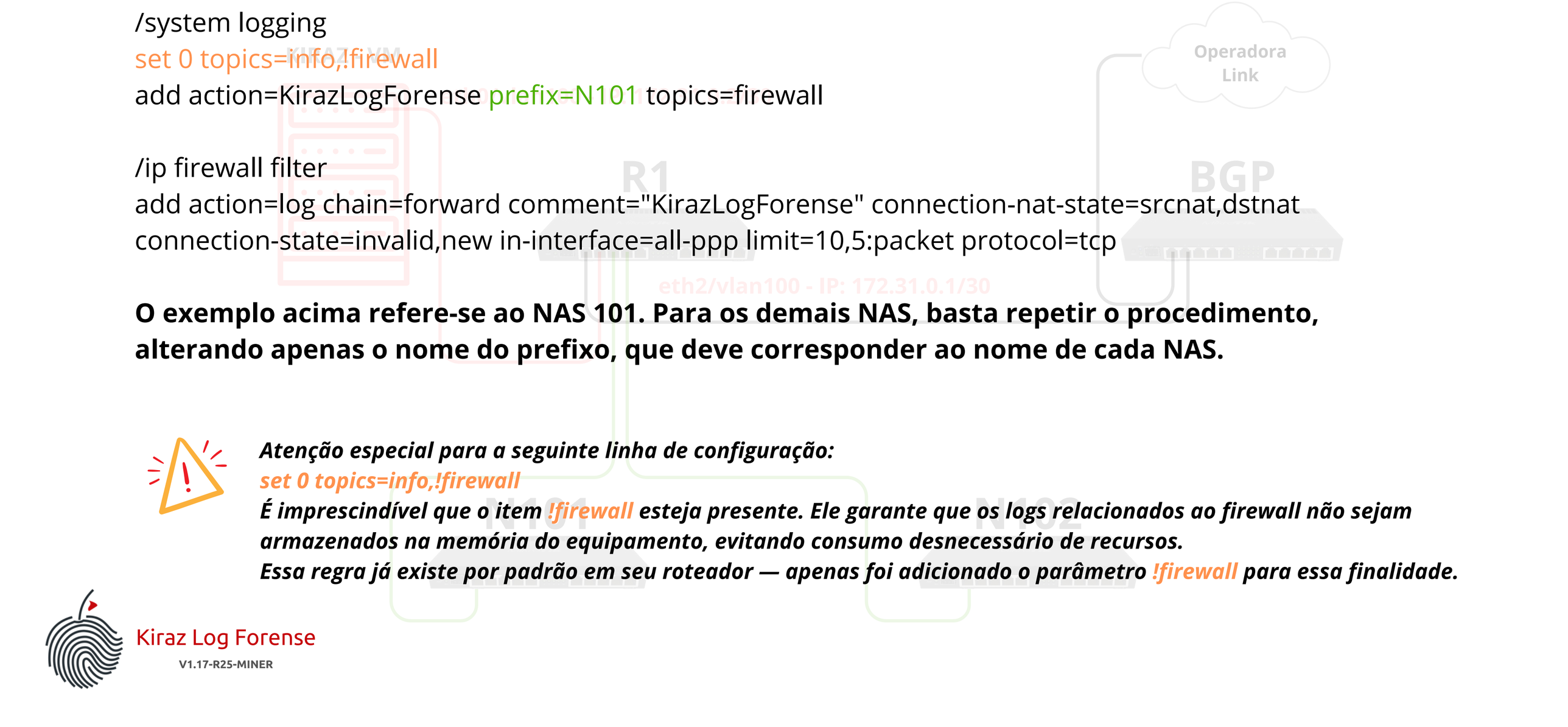
/ip firewall filter
add action=log chain=forward comment="KirazLogForense" connection-nat-state=srcnat,dstnat
connection-state=invalid,new in-interface=all-ppp limit=10,5:packet protocol=tcp

O exemplo acima refere-se ao NAS 101. Para os demais NAS, basta repetir o procedimento, alterando apenas o nome do prefixo, que deve corresponder ao nome de cada NAS.

Atenção especial para a seguinte linha de configuração:
set 0 topics=info,!firewall
É imprescindível que o item !firewall esteja presente. Ele garante que os logs relacionados ao firewall não sejam armazenados na memória do equipamento, evitando consumo desnecessário de recursos.
Essa regra já existe por padrão em seu roteador — apenas foi adicionado o parâmetro !firewall para essa finalidade.

Topologia

all-pppoe-mikrotik



Topologia

all-pppoe-mikrotik

Por fim, utilize o comando exit para sair da seção devices e, em seguida, inicie a coleta de logs e gravação para o dispositivo de ID 1, que cadastramos com o nome "todos".

A partir desse momento, o sistema estará coletando e gravando os logs. Para interromper o processo, utilize o comando stop. Caso a coleta deva continuar em segundo plano, recomenda-se apenas fazer logout.

Agora, você pode acompanhar tudo diretamente pela interface web, no menu Dashboard e Logs Forense.

```
[admin@KirazLogMiner] > devices
[admin@KirazLogMiner] (devices) > list verbose
Lista de Devices (Modo Verbose):

ID:          1
Name:        todos
Protocol:    UDP
Port:        514
IP Address:  -
User:        -
Password:    -
RemotePort:  -
VendorID:    1 (Mikrotik_ALL-PPP)
Enabled:     Yes
Description: -
---------------------------------------
[admin@KirazLogMiner] (devices) > exit
[admin@KirazLogMiner] >
[admin@KirazLogMiner] > start device_id=1
Arquivo de config gerado: /kiraz/system/miner_config.json
Conectado ao banco de dados: /kiraz/kiraz_logs/2025-04-30_16.db
 -> Threads de mineração iniciadas a partir do arquivo de config.
[admin@KirazLogMiner] start | miner > [Dev 1] todos (UDP) Porta=514, listen_only=False
```

Finalização

Dicas importantes:

1. Sempre finalize suas atividades com o comando **logout** para garantir o encerramento correto da sessão na CLI.
2. Você pode utilizar o comando **listen** com a sintaxe **start device_id=1 listen**. Nesse modo, o sistema apenas escuta a porta do dispositivo e exibe os logs na tela, o que é útil para verificar se os dados estão sendo recebidos pelo Kiraz.
3. Logs com cor ***amarela*** indicam que estão sendo recebidos corretamente.
4. Logs com cor ***vermelha*** indicam possíveis erros nas regras aplicadas ou problemas com o token do vendor.
5. Sempre que precisar encerrar o processo iniciado com **start**, utilize o comando **stop**. Comandos como Ctrl+C não funcionam no sistema. Mesmo com a tela rolando, digite stop para finalizar corretamente.
6. Quando utilizar o modo **start** sem o parâmetro **listen**, os logs não aparecerão na tela. Isso é intencional, para evitar estouro de buffer ou uso excessivo de memória RAM durante coletas prolongadas.

Bom trabalho! Aproveite o que há de melhor em armazenamento e análise de logs forenses com o Kiraz.