Solução de alerta dinâmico no monitoramento de tráfego através de fluxos de dados

Trabalho de Conclusão do Curso de Tecnologia em Sistemas para Internet

Otacir Fernando Silva
Orientador: César Augusto Loureiro

[1]Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul (IFRS)
Campus Porto Alegre
Av Cel Vicente, 281, Porto Alegre – RS – Brasil

2020000217@aluno.poa.ifrs.edu.br, cesar.loureiro@poa.ifrs.edu.br

Resumo. *A governança em redes de computadores é essencial diante da crescente complexidade dos ambientes em rede e da necessidade de comunicações seguras. Essa demanda é impulsionada pela frequência e sofisticação dos ataques cibernéticos, tornando prioritária a proteção das infraestruturas. Este artigo apresenta uma solução para os desafios na gestão de redes, com foco na detecção e alerta de anomalias. A proposta integra-se ao sistema de coleta e análise de tráfego NfSen, configurado para gerar alertas automáticos via e-mail sempre que os valores de tráfego ultrapassam um limiar percentual pré-estabelecido. A solução foi validada no Ponto de Presença da Rede Nacional de Ensino e Pesquisa (POP-RS/RNP), analisando o tráfego de rede e monitorando fluxos NetFlow, que em caso de fluxo anômalo, o sistema envia um e-mail ao administrador com os detalhes do tráfego e o horário do incidente.*

1. Introdução

Os sistemas de gerenciamento de redes desempenham um papel fundamental na administração de infraestruturas de comunicação, sendo responsáveis por monitorar, analisar e reportar o desempenho da rede. Contudo, as informações produzidas por esses sistemas são altamente sensíveis e sua exposição a ameaças pode gerar vulnerabilidades críticas, comprometendo a utilização, a estabilidade e, principalmente, a confiabilidade da rede. Tais riscos tornam indispensável o investimento em mecanismos de monitoramento eficazes para a detecção de anomalias e proteção contra incidentes de segurança.

Nesse cenário, o monitoramento de tráfego surge como uma estratégia crucial, pois permite identificar comportamentos anômalos que podem indicar ataques ou falhas. Diversos softwares estão disponíveis para essa finalidade, sendo o NfSen uma das ferramentas amplamente utilizadas. O NfSen é uma interface de análise e visualização de dados baseada no NetFlow, um protocolo que coleta informações detalhadas sobre os fluxos de tráfego na rede. Contudo, apesar de sua utilidade, o NfSen não oferece controle de alerta adaptativo, ou seja, a configuração de alertas baseados em percentuais do tráfego recebido.

Este trabalho propõe uma solução que integra alertas ao NfSen, permitindo o estabelecimento automático de limiares de tráfego e a geração de notificações em eventos críticos. Para justificar a relevância da solução, no tópico 2 desenvolve-se uma

fundamentação teórica sobre os conceitos de monitoramento e segurança em redes, seguida no tópico 3 com uma análise das ferramentas de monitoramento. A metodologia e a solução proposta são apresentadas nos tópicos 4 e 5, respectivamente, enquanto o tópico 6 aborda a validação do sistema desenvolvido e as conclusões obtidas são encontradas do tópico 7. O objetivo é fornecer uma ferramenta eficiente e adaptativa, que contribua para aumentar a segurança e a confiabilidade das redes monitoradas.

2. Fundamentação

A prática da monitorização e caracterização do tráfego de dados em redes é uma atividade rotineira no gerenciamento de sistemas de rede. Esse acompanhamento do tráfego concentra-se nas características globais do fluxo de dados na rede, desempenhando um papel crucial no gerenciamento e planejamento de redes de computadores. ”O monitoramento de um fluxo de tráfego é chamado controle de tráfego.”(Tanenbaum, 2016, p309). São essas medições que podem ser conduzidas pelos dispositivos pelos quais o tráfego naturalmente flui, como roteadores e *switches*, ou por equipamentos externos que recebem cópias de pacotes ou informações sobre os fluxos que circulam na rede.

Os conceitos de NetFlow e IPFIX são fundamentais para compreender como funciona o monitoramento de tráfego em redes de computadores. O NetFlow é um protocolo desenvolvido pela Cisco para coletar informações detalhadas sobre os fluxos de dados que trafegam em uma rede. Um ”fluxo”pode ser entendido como uma conexão ou comunicação entre dois dispositivos, identificada por informações como endereços IP, portas, protocolo utilizado e volume de dados transferidos. Essa coleta permite analisar padrões de uso, detectar anomalias e gerar estatísticas importantes para a gestão da rede (*InternationalIT*, 2024).

O IPFIX (Internet Protocol Flow Information Export) é uma evolução do NetFlow, padronizada pela IETF (Internet Engineering Task Force), que amplia suas funcionalidades. Ele oferece maior flexibilidade na definição das informações coletadas, suportando diversos tipos de dados além dos tradicionais do NetFlow. Ambos os protocolos são amplamente utilizados para o monitoramento de redes e fornecem uma base sólida para ferramentas especializadas, como o NfSen.(*InternationalIT*, 2024).

O NfSen é uma interface que utiliza dados coletados via NetFlow ou IPFIX para visualizar, analisar e interpretar o tráfego de rede. Ele auxilia administradores na identificação de possíveis problemas ou ataques. No entanto, ferramentas como o NfSen ainda possuem limitações, como a ausência de um controle adaptativo para criação de alertas personalizados baseados em percentuais de tráfego.

O NetFlow utiliza um método para consolidar o tráfego em fluxos, geralmente usando as tuplas: endereço IP e porta de origem, endereço IP e porta de destino e protocolo. Ele transmite apenas as informações estatísticas agregadas (por exemplo, quantidade de pacotes e bytes do fluxo) para uma máquina coletora (CISCO, 2024). A informação fornecida sobre cada fluxo pelo NetFlow é denominada registro de fluxo. Uma das vantagens desse método é a redução significativa da quantidade de informação que precisa ser processada pela máquina coletora, uma consideração crucial nas velocidades multigigabit dos tempos atuais.

Para receber esses fluxos e permitir a análise, existem diversos aplicativos, sendo o NfSen a ferramenta *open-source* mais utilizada, monitorando e analisando o tráfego de

rede que utiliza dados de fluxo gerados pelo NetFlow, IPFIX e SFLOW (formato de fluxo proprietário do fabricante Juniper). O NfSen permite a visualização e análise detalhada do tráfego de rede, facilitando a identificação de padrões de uso e com isso a detecção de anomalias, tais como tentativas de ataque ou tráfego indesejado, bem como o monitoramento do desempenho geral da rede. A importância do NfSen reside em sua capacidade de fornecer *insights* valiosos sobre o comportamento do tráfego, permitindo que administradores de rede tomem decisões baseadas em seus gráficos. A organização da estrutura de funcionamento do NfSen está destacada na Figura 1, que representa a estrutura de diretórios do NfSen, organizados a partir do diretório base (BASEDIR) (NfSen.Sourceforge,2024).

etc (CONFDIR): Contém os arquivos de configuração do NfSen, como o arquivo nfsen.conf, que define os parâmetros operacionais.

bin (BINDIR): Armazena os executáveis do sistema, como nfsen e nfsend, que são responsáveis pela execução e operação do NfSen.

libexec (LIBEXECDIR): Contém módulos do NfSen escritos em Perl (.pl), utilizados para processar os dados coletados.

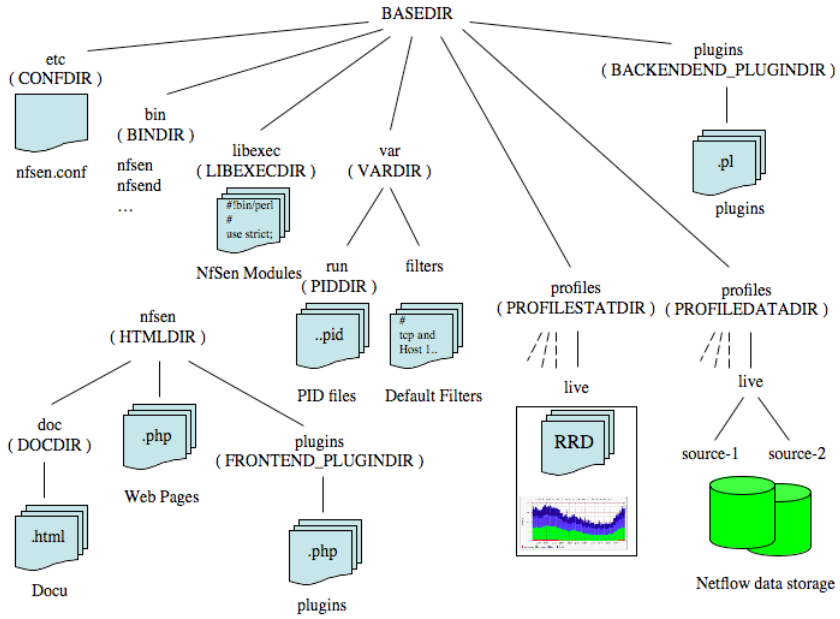
var (VARDIR): Abriga subdiretórios importantes:

run (PIDDIR): Armazena arquivos .pid, que identificam processos ativos do NfSen.

filters: Contém filtros padrão que definem critérios de seleção dos dados de tráfego. profiles: Dividido em dois subdiretórios: PROFILESTATDIR: Guarda estatísticas dos perfis.

PROFILEDATADIR: Armazena os dados coletados, organizados em fontes de tráfego (*e.g., source-1, source-2*) e representados em arquivos RRD (*Round-Robin Database*) para geração de gráficos.

Figura 1 - Estrutura de Diretório do NfSen



Fonte: https://nfsen.sourceforge.net/(2024)

O NfSen é uma ferramenta de monitoramento de rede que utiliza a linguagem *Perl* para processar dados de tráfego capturados de roteadores. Funciona em conjunto com o *nfdump*, que é uma ferramenta de coleta, processamento e análise de dados de fluxo de rede por linha de comando. Esses dados de fluxo são então transformados pelo NfSen em estatísticas, como volumes de tráfego e contagem de pacotes, e armazenados em arquivos no formato RRD (*Round-Robin Database*). O *"round robin"* se refere ao fato de que o banco de dados mantém um tamanho fixo; assim, à medida que novas entradas são adicionadas, as mais antigas são descartadas.

O NfSen gera os arquivos RRD, os quais são lidos pela ferramenta RRDTool, coletando dados de tráfego ao longo de um período fixo de tempo e removendo as informações que ultrapassam esse limiar pré-estabelecido. Assim, tem-se uma gestão eficiente do armazenamento, garantindo-se que apenas dados relevantes e recentes sejam mantidos para análise e visualização.

> "RRDtool é o padrão da indústria *OpenSource*, sistema de registro de dados e gráficos de alto desempenho para dados de séries temporais. RRDtool pode ser facilmente integrado em *scripts shell, perl, python, ruby*, lua ou aplicativos tcl."(Oetiker, 2024).

O RRDTool é essencial para armazenar e visualizar dados de séries temporais, como métricas de uso de rede, desempenho de sistemas e tráfego de servidores. (R. Views, 2018). Cada métrica é armazenada de forma circular, o que significa que novos dados substituem os antigos quando o limite de armazenamento é atingido, garantindo eficiência no uso de espaço. Além disso, é frequentemente utilizado para gerar relatórios e alertas.

O *Swaks* é uma ferramenta de linha de comando usada para testar e depurar servidores SMTP (protocolo de envio de *e-mails*). Ele permite enviar *e-mails* personalizados de maneira simples, oferecendo opções para especificar remetente, destinatário, conteúdo, autenticação, e outros parâmetros. É muito utilizado para verificar a configuração de servidores de *e-mail*, identificar problemas ou validar funcionalidades, sendo útil para administradores de sistemas e redes (Kali, 2024).

Neste trabalho, foi utilizado o NfSen para análise de tráfego de rede, integrando as ferramentas RRDTool e *Swaks*. O RRDTool é empregado para a leitura dos dados geridos pelo NfSen, permitindo uma análise aprofundada de métricas e identificação de anomalias ao passo que o *Swaks* automatizou o envio de notificações e relatórios de eventos críticos por *e-mail*, assegurando a eficiente comunicação de alertas gerados pelo sistema de monitoramento.

3. Ferramentas de Monitoramento

Segundo o site AIMultiple (2024) "*Top 7 Network Bandwidth Monitoring Software 2024*", foram selecionados os sete melhores softwares de monitoramento de banda de rede, sendo os três primeiros colocados, as seguintes ferramentas: 1. *PRTG Network Monitor* para otimização do desempenho da rede; 2. *SolarWinds Network Bandwidth Analyzer Pack*; 3. *ManageEngine Site24x7* para a plataforma de monitoramento de largura de banda. Pode-se comparar suas principais propriedades no Quadro 1:

Comparativo Softwares de Monitoramento

Ferramenta	Características	Prós	Contras
PRTG Network Monitor	Monitoramento de redes, servidores, aplicações e dispositivos. Sensores personalizáveis e alertas em tempo real.	Interface amigável, fácil de configurar, ampla personalização de sensores, possui versão gratuita limitada.	Pode ser custoso para redes maiores devido ao modelo de licenciamento por sensor.
SolarWinds Network Bandwidth Analyzer Pack	Inclui Network Performance Monitor e NetFlow Traffic Analyzer. Focado em análise de largura de banda, desempenho e detecção de problemas de rede.	Muito robusto para redes grandes, visualizações detalhadas, recursos avançados de monitoramento e análise.	Configuração inicial complexa e custo elevado para empresas menores.
ManageEngine Site24x7	Solução de monitoramento em nuvem que cobre infraestrutura, servidores, websites, e aplicativos.	Fácil de usar, bom custo-benefício, baseado em nuvem, ideal para organizações menores ou sem infraestrutura local.	Funcionalidades avançadas podem exigir integração com outras ferramentas ManageEngine; versão offline limitada.

Quadro 1 - Fonte: elaborado pelo autor (2024)

O *PRTG Network Monitor, SolarWinds Network Bandwidth Analyzer Pack e ManageEngine Site24x7* são ferramentas de monitoramento de redes robustas, cada uma com características que atendem diferentes perfis de usuários e necessidades de rede. O *PRTG Network Monitor* destaca-se pela flexibilidade e intuitividade de sua interface, sendo especialmente indicado para pequenas e médias empresas que buscam um monitoramento eficaz sem exigir conhecimentos avançados para a configuração. É um software que oferece uma estrutura de licenciamento baseado em sensores, o que permite uma adaptação personalizada para monitoramento de vários dispositivos e aplicativos, além de suportar alertas avançados e relatórios detalhados. (PRTG Network, 2024).

Por outro lado, o *SolarWinds Network Bandwidth Analyzer Pack* é uma ferramenta que oferece uma ampla gama de funcionalidades de análise de tráfego e largura de banda. Com integração ao *SolarWinds NetFlow Traffic Analyzer*, permite uma visão profunda do uso de largura de banda por aplicativo e usuário, sendo altamente customizável para redes de grande escala. (SolarWinds, 2024).

O *ManageEngine Site24x7* traz um monitoramento centrado em redes e servidores, permitindo supervisão de serviços em nuvem e ambiente de aplicativos web, mas com menos opções de personalização de alertas em comparação com o SolarWinds. (ManageEngine, 2024).

Uma questão a ser observada é que essas ferramentas possuem criação de alerta, porém não são adaptativas. Isto quer dizer, resumidamente, que não permitem a criação de alertas de forma percentual em relação fluxo recebido. Além do mais, são ferramentas comerciais que possuem custos.

4. Metodologia

O presente artigo foi desenvolvido com base em uma metodologia de pesquisa que combina aspectos qualitativos e exploratórios, focando-se em entender os principais conceitos e aplicações do NfSen no monitoramento de tráfego de rede. A abordagem qualitativa foi escolhida para possibilitar uma compreensão profunda dos fenômenos envolvidos, enquanto a pesquisa exploratória permitiu o levantamento de informações iniciais sobre o tema, oferecendo um panorama amplo e detalhado dos principais trabalhos relacionados. Como procedimento metodológico, foi adotada a pesquisa bibliográfica, com o objetivo

de fundamentar teoricamente a análise do uso do NfSen em ambientes de rede. (Prodanov; Freitas, 2013).

Além da pesquisa bibliográfica, o desenvolvimento do projeto foi realizado no ambiente do Ponto de Presença da Rede Nacional de Ensino e Pesquisa (POP-RS/RNP) do Centro de Processamento de Dados da Universidade Federal do Rio Grande do Sul - CPD/UFRGS, onde foi possível monitorar o tráfego de rede da referida instituição. Esse ambiente propiciou uma observação prática e direta dos fluxos de dados e de possíveis anomalias, essenciais para o estudo das possíveis ameaças. A análise do tráfego foi realizada com o auxílio de ferramentas específicas para coleta e visualização de dados, permitindo uma compreensão mais detalhada do comportamento da rede e das características dos diferentes tipos de tráfego.

Para estruturar o desenvolvimento da solução proposta, foi adotado o modelo em cascata, um processo clássico de software que segue estágios discretos de especificação, projeto, implementação, teste e manutenção. Embora o modelo seja linear, permitindo que cada fase seja concluída antes do início da próxima, também houve interações entre os estágios, especialmente durante o teste e a implementação. Esse processo garantiu uma base sólida para a continuidade e a evolução do sistema, possibilitando ajustes ao longo do desenvolvimento, conforme foram surgindo novas demandas e descobertas. (Sommerville, 2011).

5. Solução Proposta

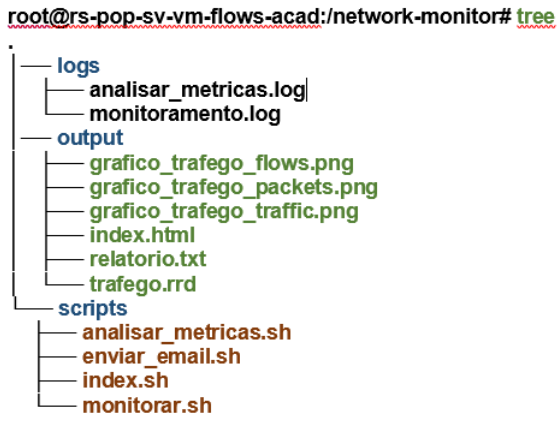
Durante o monitoramento, o NfSen utiliza a ferramenta RRDTool para geração de gráficos em tempo real, utilizando o comando *rrdtool graph*, que exibe visualmente as métricas de desempenho, facilitando a análise e o acompanhamento do sistema ao longo do tempo. Esta aplicação permite o uso de *scripts* automáticos que alimentam continuamente o banco de dados, realizando coletas regulares de métricas de rede.

Para realizar a leitura dos arquivos RRD, é necessário o uso do comando *rrdtool fetch*, que extrai informações registradas em intervalos específicos. No caso do monitoramento de IPv6, o NfSen organiza perfis e armazena as métricas de tráfego separadamente para cada cliente, utilizando diretórios específicos para cada perfil. Isso permite uma gestão detalhada e individualizada do tráfego de cada cliente.

A fim de atingir a solução de geração de alertas adaptativos, foram criadas uma série de comandos que monitoram a ferramenta NfSen. A estrutura do diretório */network-monitor* foi dividida em subdiretórios denominados de *logs*, *output* e *scripts*.

No subdiretório *logs* armazena-se os arquivos de *log* gerados durante o monitoramento e execução dos *scripts*, registrando informações sobre o processo e eventuais erros. O subdiretório *output* contém os resultados e relatórios gerados pelo programa, como gráficos e relatórios de análise de dados, e o último subdiretório, o *scripts*, guarda a sequência de comandos responsáveis pela coleta de dados, análise e geração de relatórios, ou seja, os arquivos executáveis que realizam a análise, o monitoramento e o processamento dos dados. A estrutura criada pode ser verificada na Figura 2.

Figura 2 - Estrutura de Diretório do Network-Monitor



Fonte: elaborado pelo autor (2024)

O sistema aciona primeiramente o comando *monitorar.sh*, conforme apresentado na figura 3, momento em que executa uma leitura de tráfego de rede e toma ações automatizadas para análise e monitoramento da rede.

Figura 3 - monitorar.sh

```
coletar_dados() {
    log_message "Iniciando coleta de dados..."

    # Coletando os dados de tráfego das últimas 12 horas
    # Dados brutos diretamente do arquivo RRD
    dados=$(rrdtool fetch $RRD_FILE AVERAGE --start -43200 --end now)

    # Salvar todos os dados brutos coletados no arquivo de log para análise futura
    echo "$dados" >> /network-monitor/logs/dados_completos.txt
}

# Atualizando arquivo RRD com os dados coletados
atualizar_rrd() {
    log_message "Atualizando arquivo RRD com os dados coletados..."

    # Atualiza o RRD com os dados brutos coletados
    # Não há necessidade de processar ou filtrar, apenas atualizar com os dados brutos
    rrdtool update $RRD_OUTPUT_FILE $dados

    # Verificar se a atualização foi bem-sucedida
    if [ $? -ne 0 ]; then
        log_message "Erro ao atualizar o arquivo RRD com os dados coletados."
        exit 1
    fi

    log_message "Finalizando a atualização."
}

# Iniciando monitoramento
log_message "Iniciando o analisar_metricas.sh..."
bash /network-monitor/scripts/analisar_metricas.sh

log_message "Atualizando os arquivo RRD."
atualizar_rrd

log_message "Monitoramento concluído com sucesso."
```

Fonte: elaborado pelo autor (2024)

Na sequência, o *script analisar-metricas.sh* é responsável por processar os dados coletados de tráfego da rede, identificar anomalias com base em limites pré-definidos, neste artigo, estabelecendo um limiar de 75% acima do último pico (configurável) como critério para identificar algum tipo de tráfego anômalo e gerar relatórios detalhados. Esses relatórios incluem gráficos e estatísticas, como pode ser observar na programação constante na Figura 4. A detecção de anomalias se dá a partir dos dados armazenados nos arquivos do (*trafego.rrd*) onde armazena os dados coletados de tráfego das últimas doze horas.

Figura 4 - analisar_metricas.sh

```
# Gerando relatório em formato de tabela
log_message "Gerando relatório..."
{
    echo "Relatório de Monitoramento - $data"
    echo ""
    echo "Métricas Coletadas"
    echo ""
    printf "%-10s %-20s %-20s %-20s\n" "Horário" "Fluxos f/s" "Pacotes p/s" "Tráfego Mb/s"
    for i in "${!horarios[@]}"; do
        # Conversão dos valores para unidades legíveis para exibição na tabela
        human_flows=$(convert_units "${flows[i]}")
        human_packets=$(convert_units "${packets[i]}")
        human_traffic=$(convert_units "${traffics[i]}")

        printf "%-10s %-20s %-20s %-20s\n" "${horarios[i]}" "$human_flows " "$human_packets " "$human_traffic "
    done

    echo ""
    echo "Anomalias Detectadas"

} > "$relatorio"

log_message "Relatório gerado com sucesso."

# Gerando gráficos para as métricas
log_message "Gerando gráficos..."


# Verificando anomalias para Fluxos, Pacotes e Tráfego
anomalia_detectada=0

# Calculando limiar de anomalia (75% acima do valor inicial para cada métrica)
limiar_fluxo=$(echo "${flows[0]} * 1.75" | bc)
limiar_pacote=$(echo "${packets[0]} * 1.75" | bc)
limiar_trafego=$(echo "${traffics[0]} * 1.75" | bc)
```

Fonte: elaborado pelo autor (2024)

Verificadas as leituras de tráfego, ocorre o registro das ocorrências no arquivo de (*relatorio.txt*). Em seguida, analisa os picos instantâneos e o tráfego dos últimos cinco minutos, disparando um alerta via *e-mail* para o administrador da rede caso anomalias sejam detectadas. Para realizar a tarefa de enviar os e-mails de alerta, foi instalada a ferramenta *Swaks (Swiss Army Knife SMTP)*, que é escrito em *perl* (interpretador/compilador) para testar as transações de configurações em SMTP (Kali, 2024).

Para efetivação do *monitorar.sh* apresentado, este deve estar inserido no crontab, que é o agendador de tarefas do *Linux*. É preciso definir quando e com que frequência ele deve ser executado, sendo que o comando *crontab -e* permite abrir e editar o arquivo de configuração de cron para o usuário atual, onde as tarefas podem ser programadas conforme a demanda necessária. Assim, cada linha especifica uma tarefa com o período de tempo respectivo a ser observado, podendo ser programada, exemplificativamente, para rodar a cada 5 minutos, sendo este o mesmo tempo que utiliza a RRDTool para processar e atualizar os dados do NfSen.

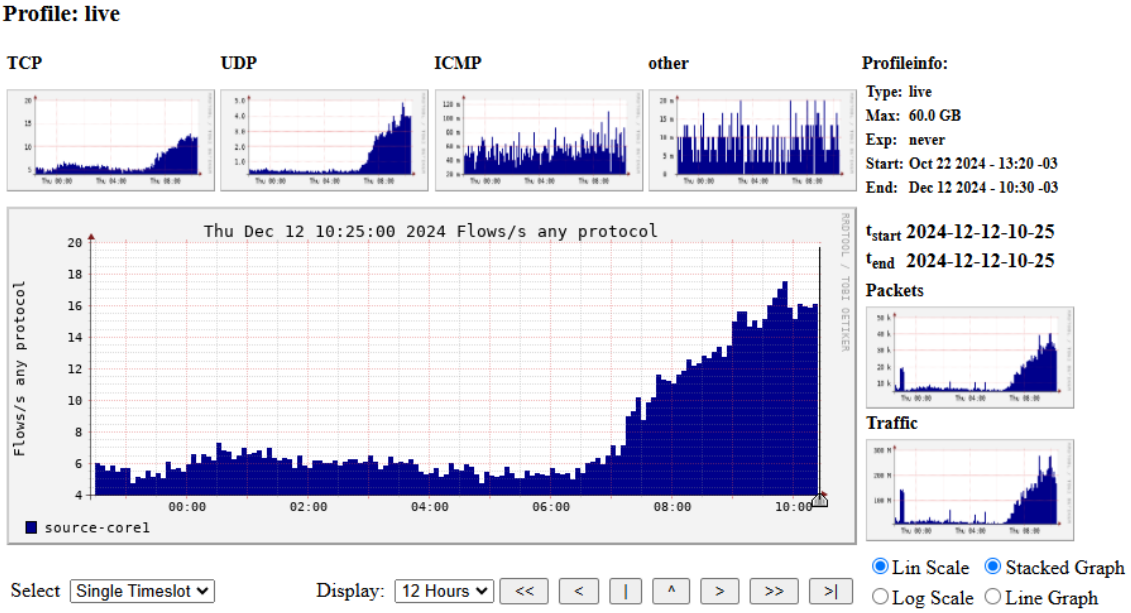
Adicionalmente à geração de alerta, é criada uma interface web para apresentar

os resultados em formato HTML (*index.sh*). O diagnóstico apresenta se há ocorrência de problema nas métricas de tráfego, fluxos ou pacotes de dados da rede, e para isso, verifica a detecção de ”anomalias”. Caso aponte algum problema, ele sinaliza com um indicador visual na cor vermelha, advertindo que algo não está dentro do padrão esperado de desempenho. Além disso, exibe gráficos que mostram como estão essas métricas ao longo do tempo, como o tráfego de dados ou o número de pacotes e fluxos na rede.

6. Validação

A solução proposta foi validada no Ponto de Presença da Rede Nacional de Ensino e Pesquisa (POP-RS/RNP), observado o tráfego de rede, conforme a Figura 4, através do gráfico de linhas do monitoramento do flows/core1.

Figura 4 - Fluxo de Rede Controles de processamento

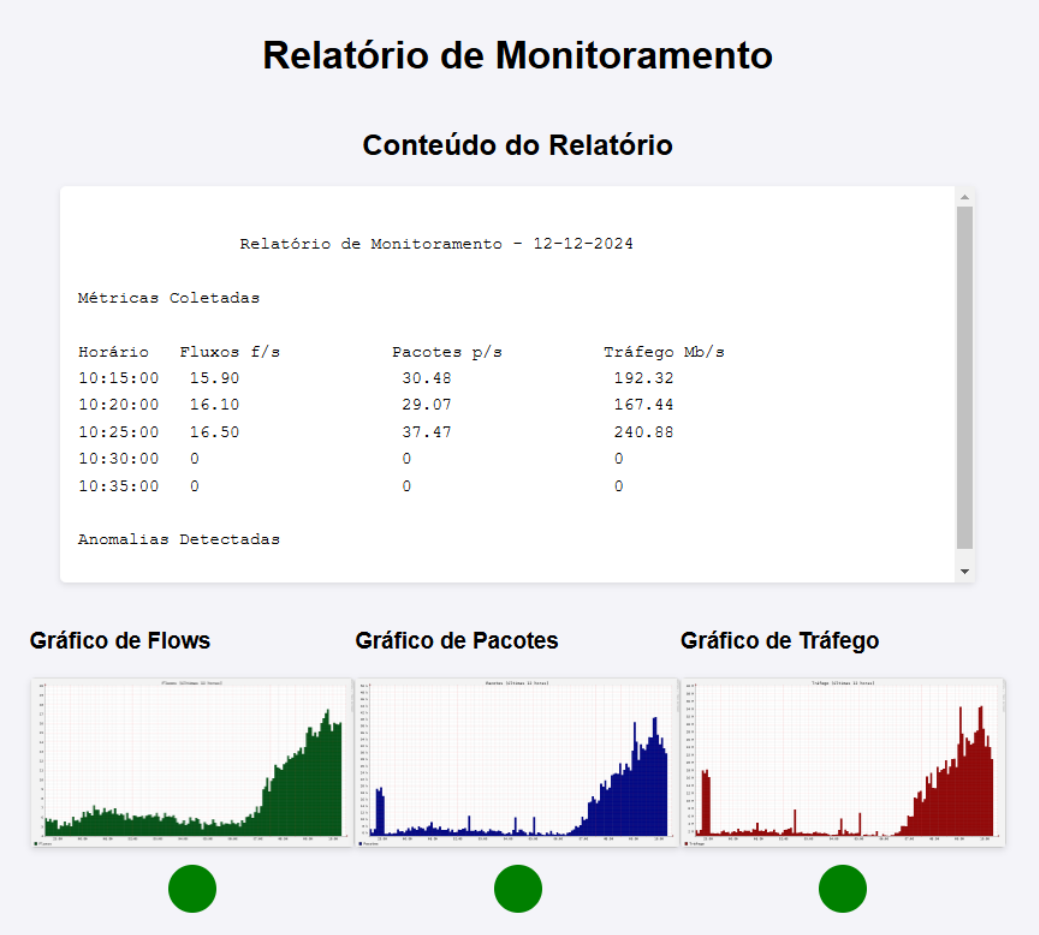


Fonte: https://flows-acad.pop-rs.rnp.br/nfsen.php (2024)

A validação envolve observar os fluxos NetFlow e verificar se a solução desenvolvida identifica a anomalia corretamente e gera o relatório correspondente. Quando um fluxo anômalo é detectado, o sistema deve enviar um e-mail ao administrador da rede com os detalhes do tráfego e o horário do incidente, conforme demonstrado no modelo abaixo, apresentando o relatório e o link para acesso aos gráficos gerados no diagnóstico prévio efetivado pelo sistema. A configuração do *script* para rodar o programa criado pelo *cron* foi definido em intervalos de 5 minutos, semelhante o utilizado pelo NfSen, permitindo que o monitoramento aconteça de forma contínua e automatizada.

Caso a verificação não apure nenhuma discrepância na análise dos dados da rede, os sinalizadores visuais permanecerão verdes; contudo, se houver alguma alteração apontada pelo software ora desenvolvido, os botões de sinalização alteram-se para a cor vermelha e o administrador recebe um e-mail com as informações no mesmo modelo, conforme se verifica na Figura 5.

Figura 5 - Relatório de Monitoramento



Fonte: elaborado pelo autor (2024)

7. Considerações Finais

Com o aumento da demanda e da complexidade nas redes de computadores, é fundamental garantir o adequado funcionamento desses sistemas, assegurando um nível mínimo de qualidade de serviço. Anomalias no tráfego de rede podem causar sérios problemas de desempenho, exigindo que os administradores identifiquem e eliminem essas irregularidades. Neste trabalho, foi proposta uma solução para a identificação automatizada desses desvios.

O programa desenvolvido para o monitoramento integrado ao NfSen desempenha o papel de interpretação dos dados de tráfego de rede. Os *scripts* foram projetados para identificar e classificar padrões de uso, além de sinalizar potenciais anomalias que possam indicar comportamentos suspeitos ou até mesmo ataques. Através de uma sequência de etapas automatizadas, os códigos verificam o volume de tráfego, calculam os picos de uso, além de armazenarem os resultados em arquivos específicos para consultas posteriores. A interface foi criada para exibir gráficos interativos, destacando variações importantes de tráfego e eventos de anomalia. Este trabalho está disponível em https://github.com/OFSilva-v2/network-monitor, para consulta e futuras melhorias.

Uma melhoria relevante seria a adoção de aprendizado de máquina para análise dos padrões de tráfego, o que permitiria identificar anomalias de forma mais precisa e

adaptativa. Por fim, o sistema poderia incluir um módulo de auditoria para registrar as ações tomadas após os alertas, facilitando a análise posterior e aprimorando a segurança e a confiabilidade do monitoramento da rede.

8. Referências

AIMultiple Research. Disponível em: https://research.aimultiple.com/network-bandwidth-monitoring-software/. Acesso em: 10 nov. 2024.

Claffy, K.; Braun, H.-W.; Polyzos, G.”A parameterizable methodology forinternet traffic flow profiling”. IEEE Journal on Selected Areas in Communications. 8ª Ed., 1995.

CISCO IOS NetFlow. Cisco Systems. Disponível em: https://www.cisco.com/web/go/netflow. Acesso em: 01 ago. 2024.

InternationalIT, Netflow e IPFIX ”Monitoramento e analise de trafego de rede”. Disponível em: https://www.internationalit.com/post/netflow-e-ipfix-monitoramento-e-analise-de-trafego-de-rede. Acesso em: 10 ago. 2024.

Kali. Disponível em: https://kali.org/tools/swaks. Acesso em: 01 out. 2024.

ManageEngine Site 24x7. Disponível em: https://www.site24x7.com/me-itom-solutions.html. Acesso em: 26 out. 2024.

Morimoto, Carlos Eduardo. ”Redes, guia prático: ampliada e atualizada”. 2ª Ed. Porto Alegre: Sul Editores, 2011.

Mota Filho, João Eriberto. ”Análise de tráfego em redes TCP/IP: utilize tcpdump na análise de tráfegos em qualquer sistema operacional”. 1. ed. São Paulo: Novatec, 2013.

NfSen - Netflow Sensor, SourceForge. Disponível em: https://nfsen.sourceforge.net/. Acesso em: 30 ago. 2024.

Prodanov, Cleber Cristiano; Freitas, Ernani Cesar. ”Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico”. 2ª Ed. Novo Hamburgo: Feevale, 2013.

PRTG Network Monitor: Software. Disponível em: https://www.paessler.com/prtg. Acesso em: 27 out. 2024.

Oetiker, Tobias. RRDTool Documentation Index. OSS Oetiker Tools, 2024. Disponível em: https://oss.oetiker.ch/rrdtool/doc/index.en.html. Acesso em: 14 set. 2024.

RStudio. Databases. R Views, 2024. Disponível em: https://rviews.rstudio.com/2018/06/20/reading-rrd-files. Acesso em: 25 set. 2024.

SolarWinds Observability. Disponível em: https://www.solarwinds.com/network-bandwidth-analyzer-pack. Acesso em: 26 set. 2024.

Sommerville, ”Ian Engenharia de Software”, tradução Ivan Bosnic e Kalinka G. de O. Gonçalves; revisão técnica Kechi Hirama. 9ª Ed. São Paulo: Pearson Prentice Hall, 2011.

Tanenbaum, A. S. ”Redes de computadores”. 5ª Ed. Pearson Education - Br, 2011.