# IMPACTO DO NÚMERO DE REGRAS DE *FIREWALL* ATIVA NO DESEMPENHO DE UM ROTEADOR

**Peter Rodrigo König[1], Marcos Henrique de Morais Golinelli[2]**
[1]Instituto Federal Catarinense – Campus Avançado Sombrio/konigdw@gmail.com
[2]Instituto Federal Catarinense – Campus Avançado Sombrio/marcos.golinelli@sombrio.ifc.edu.br

***Resumo:*** *Este trabalho tem como objetivo analisar o impacto do número de regras de firewall no consumo de recursos de processamento e capacidade de encaminhar pacotes de um roteador, para realização deste trabalho foram utilizados dois computadores interligados por um roteador RouterBoard 433, realizando testes de throughput com o software IPERF, os testes foram executados no modo simplex e duplex, sendo cada teste realizado sem regras, com 60, 120 e 180 regras de firewall ativas, onde foram obtidas taxa de transferência de dados e consumo de CPU do roteador. Os dados apresentados apontam que o número de regras afetam consideravelmente o desempenho do dispositivo, sendo que, quanto maior o número de regras, menor o desempenho, desse modo, tais regras devem ser elaboradas de forma criteriosa para que o dispositivo não se torne um gargalo no desempenho da rede, em casos em que exista a necessidade de um grande número de regras e alta taxa de transferência, a escolha do roteador / firewall deve levar em consideração a capacidade do hardware.*

***Palavras-Chave:*** *Desempenho de Firewall; Avaliação de Desempenho; consumo CPU firewall;*

## 1 INTRODUÇÃO

A utilização das redes de computadores e da internet está cada vez mais integrada as atividades cotidianas, seja no trabalho, ou no lazer. Para enviar e receber informações entre este universo digital são empregados diversos dispositivos, tais como switchs, *router*s, *Access Points (AP)* entre outros, que permitem a conexão dos dispositivos para o envio e recebimento de informações. Algumas redes, possuem necessidades especiais relacionadas à segurança das informações que são enviadas e recebidas, nesse contexto entram dispositivos que implementam controles de acesso, um destes é o *firewall.*

O *firewall* pode ser definido como um “sistema ou combinação de sistemas que protege a fronteira entre duas ou mais redes” (ABNT 2005, p.viii), também nas palavras de Kurose e Ross “um *firewall* é uma combinação de hardware e software que isola a rede interna de uma organização da Internet em geral, permitindo que alguns pacotes passe e bloqueando outros” (2010, p.535).

A partir das regras inseridas no *firewall*, será decidido quais os pacotes que podem ou não passar de uma rede para outra. As regras podem ser elaboradas utilizando os endereços de origem ou destino, protocolos ou portas, pacotes que não se encaixam nas regras, podem ser descartados ou encaminhados conforme a politica adotada.

O *firewall* pode ser implantado em dispositivos específico para desempenhar tal função, porém, um roteador pode desempenhar sua função de encaminhar pacotes em

conjunto com a filtragem, nesse contexto, o exercício de mais de uma função, pode proporcionar um aumento do uso da unidade central de processamento (CPU) do ativo.

Em um determinado ambiente, a lentidão e possíveis perdas no encaminhamento de pacotes podem estar relacionado a quantidade de regras de *firewall* empregadas no dispositivo.

Para medir a capacidade de transmissão de um canal de comunicação, pode-se utilizar softwares geradores de tráfego como o IPERF, que funciona em modo cliente/servidor, sendo o servidor responsável por responder as solicitações de testes iniciado pelo cliente. Este software foi desenvolvido pelo NLANDR/DAST (National Laboratory for Applied Team) em meados do ano 2000 (IPERF, 2017). Sua função era a medição do rendimento da banda de redes de computadores utilizando os protocolos TCP (Transport Control Protocol) e UDP, o IPERF utiliza como padrão o protocolo TCP, mas pode-se utilizar UDP, adicionando parâmetros na realização de medições.

Em sua instalação inicial no Linux ele opera em modo texto através do terminal. A motivação na escolha do IPERF deve-se a sua ampla utilização por profissionais de TI(Tecnologia da Informação), sua capacidade de realizar testes com diversos parâmetros, facilidade de uso e ser *open source*.

Este trabalho apresenta a seguinte pergunta de pesquisa: “qual o impacto do número de regras de *firewall* no desempenho de um roteador*?*”. Para responder esta questão, este trabalho tem como objetivo implementar um ambiente de rede composto por dois computadores em redes distintas, conectados a um roteador que exerce também a função de *firewall*, gerando trafego de pacotes entre os *hosts*, a fim de coletar os dados gerados através do software IPERF para análise do desempenho do dispositivo em relação a quantidade de regras implementadas.

## 2 METODOLOGIA

Para execução dos testes neste trabalho foram utilizados um notebook e um *desktop*, o notebook utilizando o software IPERF como cliente, possui sistema operacional GNU/Linux distribuição Debian Jessie, com: processador Intel I3, 4Gb de memória RAM e interface de rede ethernet Intel 100/1000 Mbits, o *desktop* utilizando o IPERF como servidor, possui sistema operacional Ubuntu 16.04, com processador Intel I7, 8Gb de memória RAM e interface de rede *ethernet* Atheros 100/1000 Mbits.

O roteador com função de *firewall* utilizado foi a RouterBoard 433 (Figura 01), que possui 64Mb de memória RAM e 64Mb de memória de armazenamento, integra o

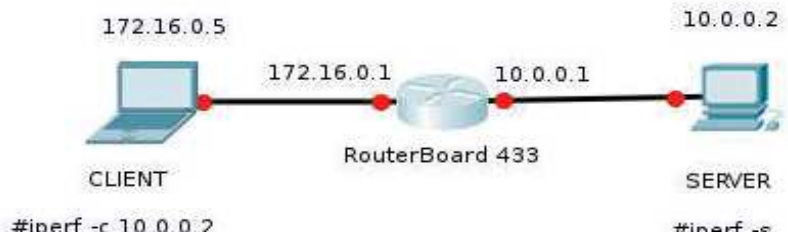
dispositivo o processador Atheros AR7130 de 300Mhz, possui 3 interfaces de rede Fast Ethernet 10/100 Mbits. Possui o sistema RouterOS Level 4 (ROUTERBOARD, 2017) , que entre diversos recursos disponíveis, está o *firewall,* onde serão adicionadas regras para realização dos testes.

**Figura 01** – Roteador Mikrotik RouterBoard 433.


Fonte: Elaboração dos autores, 2017.

A topologia empregada nos testes ilustrada na Figura 02, consiste em duas redes com endereçamento IP distinto, interligados pela RouterBoard, foi utilizando cabo de par trançado categoria 6.

**Figura 02** – Topologia




Fonte: Elaboração dos autores, 2017.

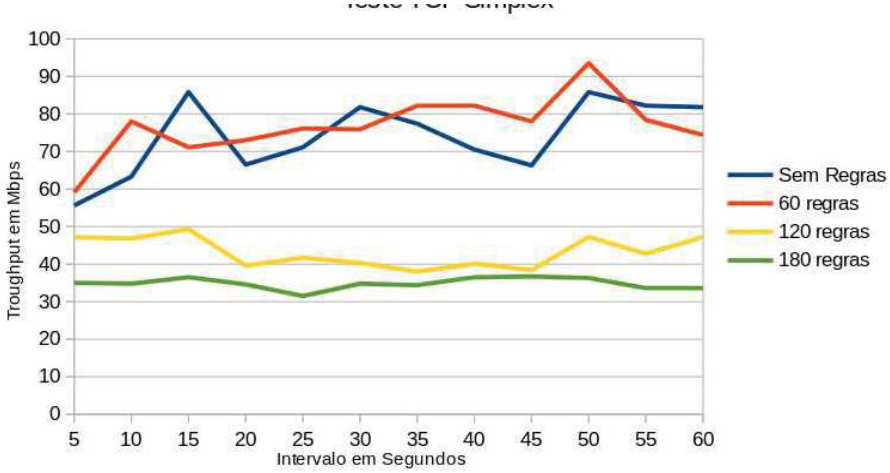
Para obtenção dos dados referente a utilização de CPU da RouterBoard, foi utilizada a API (*Application Programmable Interface)* disponibilizada pelo fabricante.

Foram realizados 4 testes para verificar a taxa de transferência (*troughtput*) entre os computadores durante 60 segundos utilizando o protocolo TCP de modo simplex (tráfego gerado em apenas uma direção) e de modo duplex (trafego gerado simultaneamente de upload e download), sendo o primeiro teste realizado sem regras de *firewall*, o segundo com 60 regras, o terceiro com 120 e o quarto teste com 180 regras para os dois modos.

## 3 RESULTADOS E DISCUSSÃO

Abaixo na Figura 03, são apresentados os resultados de *throughput* em Mbps (Megabits por segundo) e na Figura 04 do consumo de CPU dos testes simplex nos gráficos.

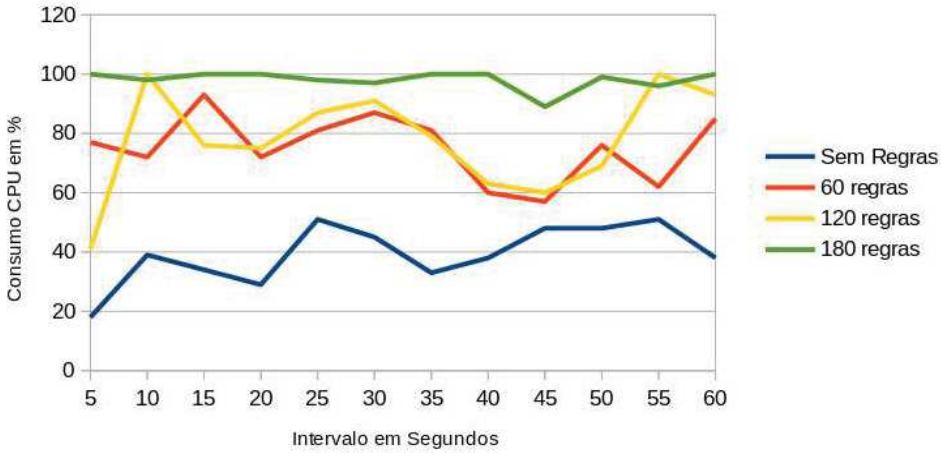
**Figura 03** – Taxa de transferência modo simplex utilizando protocolo TCP.




Fonte: Elaboração dos autores, 2017.

O teste realizado sem regras e com 60 regras possuem resultados próximos, já os testes com 120 e 180 regras apresentam uma expressiva diminuição na capacidade de transferência, sendo o teste com 120 regras obtendo uma taxa com variação entre 38 e 49,3Mbps, já o teste com 180 regras obteve uma taxa entre 31,5 e 36,7 Mbps.

**Figura 04** – Utilização de CPU no teste simplex utilizando protocolo TCP.



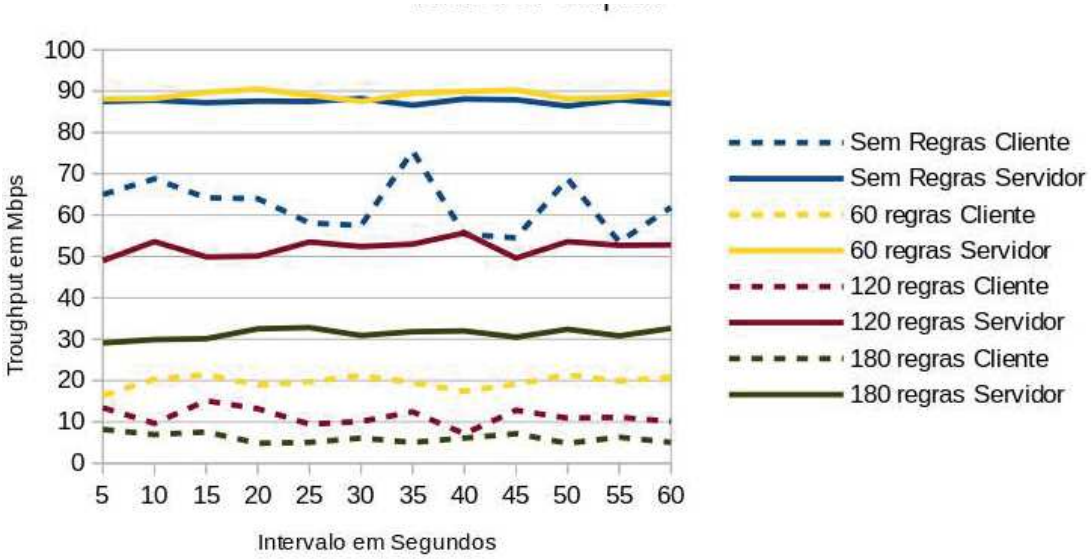

Fonte: Elaboração dos autores, 2017.

O teste sem regras de *firewall* apresenta o menor consumo de CPU, já os testes com 60 e 120 regras apresentam consumo mais elevado com médias de 75,2% e 77,8% respectivamente, o último, com 180 regras, durante quase todo o teste utilizou 100% de processamento com média de 98%.

Os próximos resultados apresentados são resultantes dos dados obtidos nos testes duplex, sendo a Figura 05 o *throughput* e a Figura 06 o consumo de CPU.

Os testes, são identificados por cores distintas, sendo que a linha tracejada representa o tráfego em direção ao cliente e a linha contínua o trafego em direção ao servidor.

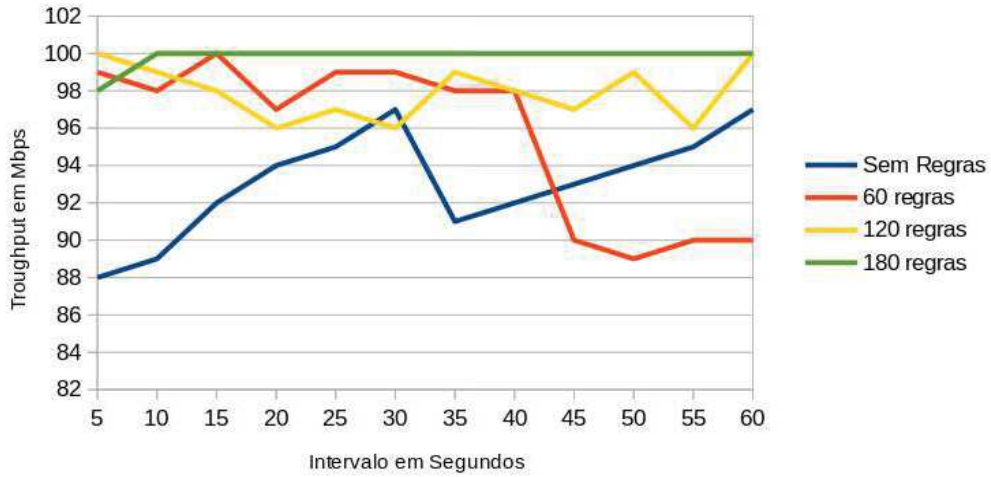
**Figura 05 –** Taxa de transferência modo duplex utilizando protocolo TCP.




Fonte: Elaborado pelos autores, 2017.

No teste sem regras, os dados obtidos apresentam médias de 87,4 e 62,2 Mbps de *throughput*, com 60 regras o valor ficou em 89 e 19,6 Mbps, o teste com 120 regras já apresenta uma degradação no desempenho, com média de 52,1 e 11,2 Mbps, o último apresentou apenas 31,2 e 6 Mbps,

**Figura 06** – Utilização de CPU no teste duplex utilizando protocolo TCP.




Fonte: Elaborado pelos autores, 2017.

Assim como no teste de tráfego que apresenta menor *throughput* com o aumento de regras, respectivamente, a demanda de CPU aumenta, com médias de 93%, 95,5%, 97,9% e 99,9% de consumo.

Os dados apresentados, indicam que quanto maior o número de regras que precisam ser processadas, maior a demanda de processamento do dispositivo, ao ponto que, ao aproximar da capacidade máxima de processamento, a quantidade de pacotes que o roteador consegue encaminhar diminui substancialmente.

Neste cenário, o roteador tornaria um ponto de gargalo na rede, sendo necessário a adoção de hardware mais potente para processar determinada quantidade de regras para obter uma taxa de transferência desejada.

## 4 CONSIDERAÇÕES FINAIS

Através dos resultados obtidos nos testes pôde-se observar que a quantidade de regras de *firewall* utilizada para proteger uma rede de computadores pode ter grande influência no desempenho dos dispositivos que trabalham realizando a filtragem de pacotes, podendo ocasionar a diminuição da quantidade de dados transferidos de uma rede a outra.

Com o apoio de ferramentas como o IPERF, profissionais de TI podem mensurar a capacidade de seus equipamentos, como apontar a necessidade da otimização na elaboração das regras de *firewall* ou a aquisição de equipamentos com hardware com maior capacidade de processamento. Também pode ser utilizado para encontrar possíveis pontos geradores de congestionamento na rede.

Como trabalhos futuros, sugere-se a utilização dos dados obtidos na modelagem de capacidade do sistema, utilizando teoria das filas, que pode ser utilizado para dimensionar modelos de previsão da capacidade de hardware necessária para atender determinado tráfego de rede com determinada quantidade de regras.

## REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27002:2005**: Tecnologia da Informação - Técnicas de Segurança - Código de prática para gestão da segurança da informação.. Rio de Janeiro: Abnt, 2005. 120 p.

BORBA, Adriano R.,CORDOVA, Mariane B., GOLINELLI, Marcos H de M. **Ferramenta IPERF para análise de desempenho de red**e. in: FREITAS JUNIOR, V.; COSTA, G. C. (Org.). Tecnologia e Redes de Computadores. 2. Ed. Sombrio: Instituto Federal Catarinense, 2016. p. 155 – 167.

IPERF. Disponível em: <https://iperf.fr/> Acesso em: 20 de abril de 2017.

KUROSE, James F., ROSS, Keith W., **Redes de computadores e a internet**. 5 ed. Trad. Opportunity translations. São Paulo : Addison Wesley, 2010.

ROUTERBOARD. Disponível em: <https://routerboard.com/rb433/> Acesso em: 20 de abril de 2017.