# IREMAC: Um IPS para Ataques Internos

Camilla Alves Mariano da Silva, Jéssica Alcântara Gonçalves, Vinicius da Silva Faria, Gabriele de Britto Vieira, Dalbert Matos Mascarenhas

***Resumo*— A diversidade dos ataques de negação de serviço criam a necessidade de avanços em ferramentas que possam reduzir os impactos relativos à inacessibilidade do serviço. Estas ferramentas em sua maioria objetivam prevenir ataques, através de medidas de contenção. O trabalho proposto, é a criação de um IPS denominado IREMAC, responsável por fazer a contenção de ataques com base nos endereços IP e MAC de máquinas situadas na rede interna. Os resultados demostram que a solução proposta apresenta desempenho satisfatório em relação ao tempo de resposta do servidor após um ataque e redução de falsos positivos que impedem comunicações legítimas.**

***Palavras-Chave*— IPS, Segurança de Redes, DoS.**

***Abstract*— The diversity of denial of service attacks create the need for advances in tools that can reduce impacts on the inaccessibility of service. These tools use techniques mostly focused on prevent attack through containment measures. The work proposed is the creation of an IPS called IREMAC, responsible for making the restriction of an attacker by IP and MAC addresses. That restriction is focuses on attacks that take place within the network. The results demonstrate that the proposed solution presents a gain in performance on server response delay after an attack and reduce false positives that prevent legitimate communications.**

***Keywords*— IPS, Network Security, DoS.**

## I. INTRODUÇÃO

Um dos principais ataques realizados na Internet, é o ataque de DoS (Denial of Service) [1]. Este ataque, pode comprometer recursos da rede, assim como hospedeiros de aplicações, como servidores de e-mail e web. Este comprometimento dos recursos pode prejudicar usuários que deveriam ter acesso aos recursos da rede. Uma parte considerável de ataques DoS consistem em estabelecer um grande número de conexões TCP semiabertas ou abertas no hospedeiro-alvo [2]. Desta forma, o hospedeiro torna-se incapaz de aceitar requisições legítimas devido ao grande número de conexões em espera, realizadas pelo ataque. Ferramentas como Ettercap [3] e t50 [4] são utilizadas para consumir os recursos de uma máquina servidora. Dentre os recursos consumidos durante um ataque, além do número de conexões em modo de espera, estão também parte da memória e do processamento. O consumo destes recursos por parte do atacante pode gerar problemas complexos relativos a disponibilidade de serviços e conteúdos por parte de seus distribuidores.

Atualmente existem diversas ferramentas e formas de ataques DoS. Dentre esses tipos de ataques, existe um que é capaz de mandar diversas requisições a um determinado servidor ao mesmo tempo forjando o endereço IP de origem. Esta técnica de forjar os endereços de origem introduz um desafio a mais na detecção da origem dos ataques de DoS. O problema é que esses endereços IP, forjados pelo atacante, podem ser inclusive endereços legítimos da própria rede em que o servidor está localizado. Desta forma os mecanismos para detecção e ou prevenção desta modalidade de ataque se torna algo crucial. Os riscos destes ataques não se restringem somente a máquinas que proveem serviços na internet, mas também a computadores ou *smartfones* de usuários. Recentes estudos mostram que até mesmo automóveis já tiveram seus serviços comprometidos através de ataques cibernéticos [5].

Dentre os mecanismos de defesa, utilizados contra ataques de DoS estão os IPSs (Intrusion Prevention System) [6]. Estes mecanismos, são capazes de detectar e bloquear ataques DoS. As funções de segurança destes mecanismos incorporam diretivas como a de filtrar o tráfego suspeito [7]. Dentre as ações de restrição de ataques utilizadas pelos IPSs, é possível bloquear ações indevidas a recursos de um servidor ou mesmo de uma rede. O IPS é capaz de identificar requisições anômalas a um servidor e gerar uma ação como por exemplo impedir que pacotes originários de um possível atacante sejam encaminhados até o destino. Uma forma de impedir essa ação é bloquear o endereço IP que esteja realizando estas requisições.

As ações restritivas de um IPS podem gerar problemas de impacto nocivos ao próprio serviço disponibilizado, como a ocorrência de falsos positivos na identificação de possíveis atacantes [8]. O falso positivo neste caso pode ter sido gerado propositalmente pelo atacante, de forma a comprometer a comunicação do servidor com usuários ou mesmo outras máquinas servidoras. Em geral, quando o atacante intenta realizar uma restrição causada por falso positivo, este pode forjar seu endereço IP de origem. Esta mudança de endereço tem como objetivo fazer com que o IPS restrinja IPs legítimos. Desta forma máquinas não maliciosas, até mesmo dentro da própria rede, seriam consideradas como potenciais ameaças e portanto teriam suas requisições bloqueadas. Com base no problema apresentado, este trabalho apresenta um IPS que além de identificar anomalias com base no IP de origem, também utiliza como base o endereço MAC(Media Access Control), o identificador único de cada dispositivo. O objetivo é tornar a detecção de intrusos mais acurada quando a mesma ocorrer dentro da própria rede e consequentemente reduzir falsos positivos.

A organização do trabalho é descrita a seguir. A seção II resume os tipos de ataques de negação de serviço e IPS. A seção III introduz uma visão sobre trabalhos que apresentam uma temática de atuação na área de prevenção e detecção de intrusos. A seção IV apresenta a ferramenta proposta

Camilla Alves Mariano da Silva, Jéssica Alcântara Gonçalves, Vinicius da Silva Faria, Gabriele de Britto Vieira, Dalbert Matos Mascarenhas, Engenharia de Computação, Centro Federal de Educação Tecnológica Celso Suckow da Fonseca (Cefet/RJ) campus Petrópolis, Petrópolis-RJ, Brasil, E-mails: calves@e-computacao.com.br, jalcantara@e-computacao.com.br,vfaria@e-computacao.com.br, gbritto@e-computacao.com.br, dalbert.mascarenhas@cefet-rj.br.

incluindo detalhes do funcionamento relativos a detecção e a tomada de decisões contra possíveis ataques. Em V, as análises comparativas entre os diferentes estágios da ferramenta e sua comparação com outra ferramenta são demonstrados em gráficos. A seção VI apresenta o resumo conclusivo das ideias e considerações propostas, bem como apresenta ideias para trabalhos futuros.

## II. Escopo de Ataques e Defesas

Os ataques de negação de serviço utilizados neste trabalho, tem como foco a inundação com requisições objetivando consumir recursos dos serviços oferecidos. Para estes ataques é utilizado um Sistema de Prevenção de Intrusos (IPS) que atua em um *gateway*, destacando-se por um IPS de redes. Um resumo dos tipos de ataques e IPS é exposto nas sub-sessões II-A e II-B respectivamente.

### A. Ataques de Negação de Serviço

Um ataque de negação de serviço (DoS) tem por finalidade tornar os recursos de um determinado sistema indisponíveis. Em muitos casos esse tipo de ataque tem como alvo servidores web, afim de impedir que usuários possam ter acesso a um determinado conteúdo. Segundo [9] existem algumas formas de negação de serviço, como consumo de recursos e exploração de vulnerabilidade. O consumo de recursos é um fator de extrema importância para um determinado serviço. Devido ao fato desses recursos como a memória e o processamento serem limitados, é possível inundar a máquina vítima com um determinado número de requisições, afim de consumir esses recursos. Esse tipo de ataque é chamado de ataque por inundação. Quando esse ataque ocorre, a vítima ou até mesmo a rede a qual está localizada fica impossibilitada de responder requisições oriundas de usuários legítimos. Para este ataque ser realizado com êxito, é fundamental que as mensagens geradas por um atacante sejam superiores à taxa que a vítima suporta. Para vítimas com alta disponibilidade de recursos, faz-se necessário um maior esforço do ataque DoS. A exploração de vulnerabilidades decorre de falhas na implementação de um protocolo, aplicação, serviço ou sistema, e também devido a problemas de configuração e administração de recursos computacionais [10]. Existe também o ataque de negação de serviço distribuído DDoS *Distributed DoS*, onde os pacotes são enviados de diferentes origens, quando um atacante sozinho não é capaz de consumir completamente os recursos da vítima [11].

### B. Sistemas de Prevenção de Intrusos

Intrusion Prevention System (IPS) é um sistema de defesa capaz de prevenir conteúdos maliciosos dentro do tráfego de rede. Ele detecta e intercepta o tráfego, tomando medidas imediatas com o objetivo de impedir ataques [12]. Segundo [13], um IPS pode tomar diversas ações, como bloqueio de portas no switch, interação com politicas de firewall externos, regras dos roteadores, ou, ainda, geração de tráfego na camada de transporte. Existem dois tipos de sistemas de prevenções de intrusos atualmente: Host-Based e InLine [14]. O baseado em host atua como a última linha de defesa, onde softwares são instalados em um determinado host que precisa de proteção. Este também é chamado de HIPS (Host Intrusion Prevention System), que consiste em um servidor de gerenciamento e um agente, que atuará entre a aplicação e o kernel do sistema operacional. Desta forma o agente tem a possibilidade de interceptar as chamadas realizadas pelo sistema ao kernel comparando com uma lista de controle de acessos definida pelo HIPS. Esta lista é utilizada para tomar decisões de permissão do tráfego em questão. Um IPS baseado em rede como o NIPS (Network Intrusion Prevention System) é um sistema localizado no gateway. Aproveitando-se deste posicionamento o NIPS irá monitorar o tráfego da rede afim de detectar e prevenir incidências de conexões maliciosas.

## III. Trabalhos Relacionados

Diversos mecanismos de defesa contra ataques DoS vêm sido propostos. Em muitos casos, a solução adotada se dá por diversos fatores, como: confiar em uma determinada lista de IP's, realizar o bloqueio de IP's considerados atacantes, gerar modelos de tráfego, dentre outros. A solução proposta por [15] analisa o tráfego de entrada e saída que chega ao roteador, afim de manter um histórico com boas conexões estabelecidas. Tendo como base essas informações, é gerada uma tabela de conexões confiáveis, para que em situações de ataque, as mesmas sejam favorecidas em detrimento à conexões desconhecidas ou ilegítimas. O trabalho de [16], consiste em interceptar os pacotes maliciosos oriundos de ataques antes que os mesmos cheguem até a máquina alvo. Isto é realizado através de uma solução de longo prazo incluindo históricos de tráfego, apelidada de *Internet Firewall Approach*. Nesta abordagem utiliza-se uma quantidade de filtros de pacotes afim de examinar se a origem e o destino procedem de ligações esperadas. Em [17], um histórico contendo todos os endereços IP legítimos é armazenado em um roteador de borda. Dessa forma, quando o mesmo encontra-se sobrecarregado, esse histórico é utilizado para tomar a decisão de aceitar ou não um novo pacote IP. Na técnica proposta por [18], um sistema distribuído é capaz de recolher dados a partir de sensores e calcular a condição da rede, afim de gerar modelos de tráfego. Se o tráfego entrante é considerado anômalo, são gerados alarmes com graus de prioridade que poderão descartar os pacotes maliciosos ou realizar um balanceamento de carga para outro servidor menos sobrecarregado e de prioridade inferior. A abordagem feita por [19], propõe um método de mineração de dados para detectar e prevenir ataques. Os autores utilizam a combinação do PfSense [20] em conjunto com o Snort [21]. A técnica utilizada inclui múltiplas formas de classificação de ataque, afim de alcançar um nível de precisão e reduzir falsos alertas.

## IV. IREMAC (IPS com Restrição de Endereço MAC)

A solução apresentada nesse trabalho, IREMAC, consiste em prevenir que um servidor de aplicação, neste caso um servidor web, tenha o seu serviço interrompido por ataques DoS. O cenário utilizado possui os servidores de aplicação dispostos em uma sub-rede distinta dos possíveis usuários.

Devido a esta distinção, para que o usuário possa fazer requisições a estes servidores, faz-se necessário a realização de um port-forward, que consiste em mascarar a porta da rede interna para a rede externa, assim como a interface de rede, realizando o NAT (Network Address Translation). A ferramenta criada é um IPS, responsável por identificar e analisar uma intrusão e bloquear possíveis tráfegos maliciosos. O IREMAC é posicionado entre as duas sub-redes, criando uma ponte entre as mesmas. O motivo desta configuração é concentrar todo tráfego no IREMAC, para que possa analisar e consequentemente tomar ações quando necessário.

O IREMAC realiza monitoramento constante à interface de rede dos hospedeiros que armazenam os serviços requerentes de proteção. Este monitoramento também se dá através do envio de requisições de pacotes sonda para a porta do serviço monitorado. Neste trabalho a porta monitorada foi a HTTP, pois os alvos de proteção são servidores WEB. O servidor web utilizado para a realização de testes foi o servidor APACHE [22]. A razão por sua escolha está diretamente ligada à popularidade deste servidor para o provimento de serviços de páginas [23].

A arquitetura proposta consiste em utilizar o IREMAC em conjunto com dois servidores WEB. Estes servidores serão protegidos e monitorados pelo IREMAC. Para descrição da arquitetura os servidores serão chamados aqui de WEB 1 e WEB 2. No primeiro momento, o IREMAC realizará o encaminhamento de requisições HTTP para o primeiro servidor, WEB 1. O WEB 2 permanece ativo porém sem entrada de tráfego. Sabendo-se que servidores WEB suportam uma quantidade limitada de conexões, de forma que, ao excedê-las, o serviço provido ficará inacessível, o IREMAC conta com um filtro de pacotes que delimitará a quantidade de conexões permitidas a cada usuário. A razão para isto está em conter ataques de DoS, com múltiplas requisições TCP, que sejam originadas de um mesmo endereço IP.

A outra forma de monitoramento é baseada no número de respostas aos pacotes sondas que IREMAC envia para os servidores direcionados às suas portas de serviços, por exemplo em um servidor HTTP, porta 80 TCP. Caso o limiar de respostas à estes pacotes sonda sejam excedidos, o IREMAC gerará um alerta de possível ataque e imediatamente assume que o servidor monitorado está sobre ataque. Paralelo a esta ação, o IREMAC analisa os logs gerados pela ferramenta tcpdump [24]. Nestes logs é feita uma análise afim de verificar a quantidade de IP's associados a um determinado endereço MAC. Caso um MAC esteja associado a mais de um endereço IP, ele é considerado malicioso e é adicionado a uma lista negra. Os endereços MACs contidos nesta lista são posteriormente bloqueados pelo servidor IREMAC como medida preventiva. O bloqueio dos MACs considerados como potenciais ameaças é feito aplicando regras ao IPTABLES [25] de forma automática.

Quando o servidor web sofre um ataque de múltiplas requisições TCP, o mesmo fica sobrecarregado e sem a possibilidade de estabelecer novas conexões por um determinado tempo. Este tempo pode variar em função do tipo de ataque e a continuidade do mesmo. A arquitetura proposta, consistindo de redundância de servidores, é planejada para

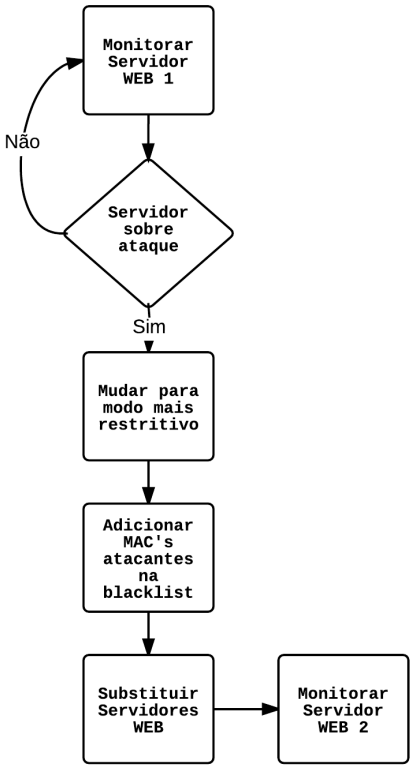


Fig. 1. Fluxograma de funcionamento do IREMAC.

que uma vez comprometido um servidor o IREMAC possa encaminhar o tráfego para o servidor redundante. Este servidor redundante tem a capacidade de permitir novas conexões e consequentemente reduzir o tempo de indisponibilidade do serviço oferecido. Desta forma, após o endereço MAC da máquina atacante ter sido adicionado à lista negra, o IREMAC faz o redirecionamento do tráfego HTTP para o servidor redundante. Nesta etapa pós ataque o servidor redundante atua como servidor WEB principal assumindo o papel de atender às requisições de páginas dos usuários. Nesse outro momento, o IREMAC atua de forma mais rigorosa, permitindo um menor número de conexões por usuário e bloqueando conexões oriundas das máquinas que foram consideradas atacantes.

A Figura 1 exemplifica o funcionamento do IREMAC na arquitetura proposta. O primeiro passo está na detecção de um possível ataque ao servidor WEB1, servidor HTTP primário, após a geração do alarme o IPS inicia sua ação de políticas mais defensivas. As configurações de defesa serão alteradas para um modo mais restritivo. Os endereços MAC's das máquinas atacantes serão adicionados à lista negra, e consequentemente após esta inserção o fluxo de ataque oriundo destas é bloqueado. Uma vez que o tráfego de ataque é mitigado, o redirecionamento do tráfego passará para o servidor WEB 2. Este atua então como novo servidor de páginas principal. Após esta etapa o IREMAC continua monitorando o servidor WEB 2, porém com a configuração mais restritiva. Nesta configuração mais restritiva o número de conexões por

endereço é reduzido e as máquinas suspeitas de ataque são adicionadas a lista negra.

## V. Resultados

Os testes do IREMAC foram realizados em um laboratório com 20 máquinas atuando na mesma rede e utilizando o IPS IREMAC como ponte para acesso aos servidores WEB. Foram realizados 10 testes para cada configuração e os resultados apresentam as médias. Foram utilizadas máquinas com o Intel Core i5 3.40GHz com 4GiB de memória, com o sistema operacional Ubuntu 15.04. Os testes aplicados ao IREMAC também foram replicados ao PfSense+Snort. Este último foi escolhido devido a sua ampla utilização no segmento de segurança da informação [19]. Nos testes o conjunto PfSense+Snort foi instalado com a configuração de IPS e com as regras padrão do Snort para ataques de DoS. Desta forma o IPS PfSense+Snort atuou como uma solução comparativa com o IPS IREMAC. O número de máquinas que realizam ataques simultâneos foi alterado para que fosse possível identificar a relação entre máquinas atacantes e o comprometimento dos recursos dos servidores WEB.

A Figura 2 demostra o tempo necessário para realizar a mudança de um servidor web para o outro. Nestes testes foram feitas requisições ao servidor web, por máquinas que simulavam requisições legítimas utilizando a ferramenta wget. As páginas são requisitadas obedecendo um limiar de requisição sucessiva. Nos primeiros testes este limiar foi de 20s e o tempo total decorrido entre as retransmissões para adquirir a página foi de aproximadamente 28,5s. Reduzindo o limiar para 5s o tempo total para adquirir uma página foi reduzido para 7,3s. Estes tempos representam uma requisição no período de troca de tráfego entre o servidor principal e o secundário. Este tempo representou um fator positivo ao objetivo de reduzir o tempo de indisponibilidade do serviço.

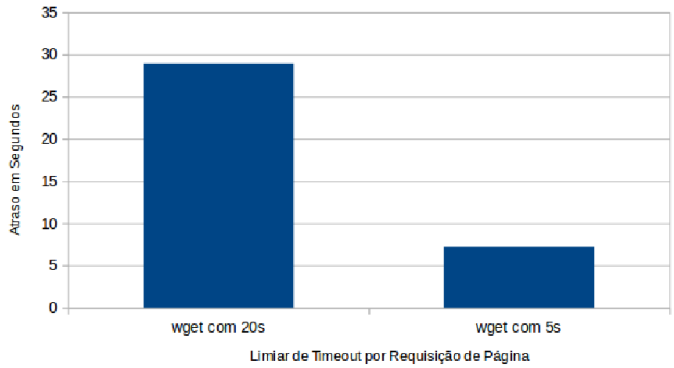


Fig. 2. Atraso médio para transição entre servidores WEB.

A Figura 3 apresenta os resultados dos ataques utilizando a ferramenta t50. Os ataques aconteceram em estágios em que apenas uma máquina atacava por vez e posteriormente esse número foi aumentando até três atacantes simultâneos. Os resultados do IREMAC com a configuração Básica, ou seja menos restritiva, apresentam uma diferença significativa com relação ao tempo total decorrido para que uma página fosse adquirida por máquinas que não eram atacantes. Quando a máquina sofre o ataque de apenas uma máquina o atraso na resposta à requisição é de aproximadamente 0,01s. No entanto aumentando o número de computadores participando de forma simultânea no ataque o atraso aumenta para 0,35s. Utilizando a configuração Restritiva do IREMAC o atraso foi reduzido para 0,0062s. Os atrasos relativos ao PfSense+Snort foram mais elevados devido aos falsos positivos em que IPs legítimos eram usados no DoS. Para estes testes o T50 foi configurado para operar em modo mais agressivo. Apesar desta configuração agressiva, observa-se que através dos registros a ferramenta cria uma grande variedade de IPs pertencentes à redes diferentes das quais os IPSs estavam. Isto consequentemente facilitou o descarte de pacotes oriundos de redes que não condiziam com a rede na qual a interface dos IPSs estavam.

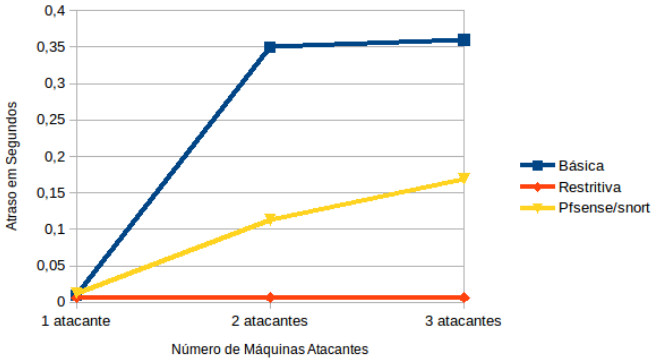


Fig. 3. Atrasos de requisição de página sob ataque da ferramenta T50.

Os resultados utilizando a ferramenta de ataque DoS, Ettercap, são apresentados na Figura 4. Nos testes o IREMAC utilizando a configuração Básica apresentou o pior desempenho, incluindo o consumo de processamento apresentado na Figura 5. Mesmo com apenas uma máquina atacante o servidor WEB é comprometido pelo ataque, o que impossibilita que seja carregada a página em tempo hábil. Este fator se deve ao Ettercap ter enviado mais pacotes em um curto espaço de tempo e também a possibilidade de utilizar IPs falsos que pertencessem a mesma rede das máquinas de usuários legítimos. O IREMAC atuando em modo Restritivo, ou seja quando o mesmo reage a um ataque, apresentou um tempo de reposta à requisição de páginas mais satisfatório. Este tempo ficou em aproximadamente 0,01s. O PfSense+Snort obteve novamente um maior atraso devido aos IPs que foram sorteados nos ataques do Ettercap. Os resultados demonstram que apesar do modo de configuração Básico do IREMAC funcionar apenas em um cenário onde ainda não existe ataque, este apresenta alta vulnerabilidade aos ataques da ferramenta Ettercap. Esta vulnerabilidade não é verificada quando o IREMAC reage com sua configuração mais restritiva.

Entretanto o PfSense/Snort apresentou falsos positivos quando os ataques de DoS são feitos variando os IPs da mesma rede onde estão as máquinas de usuários legítimos. O motivo pelo qual isto aconteceu se deve ao modo de funcionamento do PfSense/Snort à ataques de DoS. Nestes ataques o PfSense/Snort bloqueia os IPs que considera

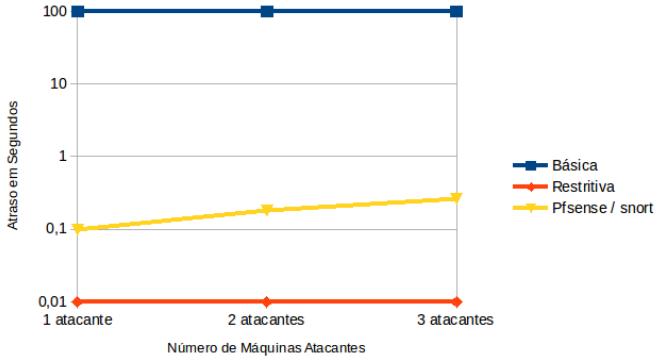


Fig. 4. Atrasos de requisição de página sob ataque da ferramenta Ettercap.

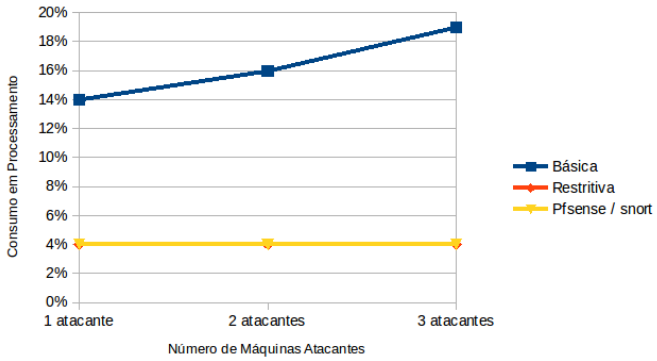


Fig. 5. Consumo de processamento na máquina servidora sob ataque da ferramenta Ettercap.

oriundos das máquinas atacantes. Este bloqueio de IPs, que em determinados casos eram de máquinas legítimas, mas que foram forjados pela ferramenta de ataque impediu as requisições legítimas. Estas requisições foram bloqueadas pois o PfSense/Snort adicionou os IPs das máquinas não atacantes à sua lista negra. Utilizando o IREMAC isto não acontece, pois o bloqueio não é feito pelo endereço IP mas sim pelo endereço MAC. Desta forma o IPS IREMAC apresenta um ganho quando utilizado como IPS para proteção de servidores dentro de redes internas.

## VI. Conclusões

Este trabalho apresentou uma forma de defesa contra ataques DoS oriundos da rede interna. A arquitetura apresentada demonstra que o IREMAC pode ser utilizado em conjunto com servidores redundantes, de forma a reduzir o tempo de inacessibilidade pós ataque. A troca do servidor que está sobre ataque por outro se mostrou eficaz quando comparado ao tempo de resposta após um ataque bem sucedido. O bloqueio de máquinas atacantes por MAC apresentou uma redução nos falsos positivos de endereços IPs de máquinas que realizam requisições legítimas. Em trabalhos futuros será analisado a criação de módulos adicionais para controle de redes sem fio de forma distribuída. Pretende-se também realizar um controle de lista negra, vinculado aos servidores de autenticação como RADIUS e consequentemente obter mais detalhes sobre a máquina que está realizando o ataque.

## Referências

[1] T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of network-based defense mechanisms countering the dos and ddos problems," *ACM Computing Surveys (CSUR)*, vol. 39, no. 1, p. 3, 2007.
[2] J. F. Kurose, K. W. Ross, A. S. Marques, and W. L. Zucchi, *Redes de Computadores e a Internet: uma abordagem top-down*. Pearson, 2010.
[3] A. Ornaghi and M. Valleri, "Ettercap," 2005.
[4] A. L. R. Corrêa and H. P. Martins, "Monitoramento de ataques de negação de serviço: Um caso prático utilizando slowloris."
[5] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *Intelligent Transportation Systems, IEEE Transactions on*, vol. 16, no. 2, pp. 546–556, 2015.
[6] P. S. Kenkre, A. Pai, and L. Colaco, "Real time intrusion detection and prevention system," in *Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014*. Springer, 2015, pp. 405–411.
[7] R. Zuech, T. M. Khoshgoftaar, and R. Wald, "Intrusion detection and big heterogeneous data: A survey," *Journal of Big Data*, vol. 2, no. 1, pp. 1–41, 2015.
[8] I. Butun, S. D. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," *Communications Surveys & Tutorials, IEEE*, vol. 16, no. 1, pp. 266–282, 2014.
[9] R. P. Laufer, I. M. Moraes, P. B. Velloso, M. D. Bicudo, M. E. M. Campista, D. d. O. Cunha, L. Costa, and O. Duarte, "Negaçao de serviço: Ataques e contramedidas," *Livro Texto dos Mini-cursos do V Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, 2005.
[10] E. T. Nakamura and P. L. Geus, *Segurança de redes*. Berkeley, 2002.
[11] R. P. Laufer, "Rastreamento de pacotes ip contra ataques de negação de serviço," Ph.D. dissertation, UNIVERSIDADE FEDERAL DO RIO DE JANEIRO, 2005.
[12] M. I. Shafi, M. Akram, S. Hayat, and I. Sohail, "Effectiveness of intrusion prevention systems (ips) in fast networks," *arXiv preprint arXiv:1006.4546*, 2010.
[13] E. Coser, "Automatização do processo de contenção de ameaças baseada em ferramenta de ids/ips (sistema de detecção e prevenção de intrusão)," 2012.
[14] S. V. B. Evangelista, "Sistemas de detecção de intrusos e sistemas de prevenção de intrusos: Princípios e aplicação de entropia," *Petrópolis: Instituto Superior de Tecnologia em Ciência da Computação*, 2008.
[15] E. Oliveira, R. Aschoff, B. Lins, E. Feitosa, and D. Sadok, "Avaliação de proteção contra ataques de negação de serviço distribuídos (ddos) utilizando lista de ips confiáveis," *VII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, 2007.
[16] R. K. Chang, "Defending against flooding-based distributed denial-of-service attacks: a tutorial," *Communications Magazine, IEEE*, vol. 40, no. 10, pp. 42–51, 2002.
[17] T. Peng, C. Leckie, and K. Ramamohanarao, "Protection from distributed denial of service attacks using history-based ip filtering," in *Communications, 2003. ICC'03. IEEE International Conference on*, vol. 1. IEEE, 2003, pp. 482–486.
[18] S. Mohiuddin, S. Hershkop, R. Bhan, and S. Stolfo, "Defending against a large scale denial-of-service attack," in *Proc. 2002 IEEE Workshop on Information Assurance and Security*. Citeseer, 2002.
[19] M. Tabash and T. Barhoom, "An approach for detecting and preventing dos attacks in lan," *International Journal of Computer Trends and Technology IJCTT Vol 18 number 6*.
[20] C. M. Buechler, J. Pingle, and J. Reed, *PfSense: The Definitive Guide: the Definitive Guide to the PfSense Open Source Firewall and Router Distribution*. Reed Media Services, 2009.
[21] M. Roesch *et al.*, "Snort: Lightweight intrusion detection for networks." in *LISA*, vol. 99, no. 1, 1999, pp. 229–238.
[22] R. T. Fielding and G. Kaiser, "The apache http server project," *Internet Computing, IEEE*, vol. 1, no. 4, pp. 88–90, 1997.
[23] Y. Diao, J. L. Hellerstein, S. Parekh, and J. P. Bigus, "Managing web server performance with autotune agents," *IBM Systems Journal*, vol. 42, no. 1, pp. 136–149, 2003.
[24] V. Jacobson, C. Leres, and S. McCanne, "The tcpdump manual page," *Lawrence Berkeley Laboratory, Berkeley, CA*, 1989.
[25] D. Hoffman, D. Prabhakar, and P. Strooper, "Testing iptables," in *Proceedings of the 2003 conference of the Centre for Advanced Studies on Collaborative research*. IBM Press, 2003, pp. 80–91.