Ataques de Reflexão Amplificada Sobre TCP Explorando Middleboxes

*Presented at the Workshop on Communication Networks and Power Systems (WCNPS'25)

Paulo Victor França de Souza
Departamento de Ciência da Computação
Universidade de Brasília
Brasília, Brasil
paulovictorfs@outlook.com

João J. C. Gondim
Departamento de Engenharia Elétrica
Universidade de Brasília
Brasília, Brasil
gondim@unb.br

***Resumo*—Ataques de reflexão amplificada sobre TCP explorando middleboxes, descritos pela primeira vez em 2021 e já observados em incidentes reais, representam uma ameaça emergente à segurança cibernética. Essa técnica abusa de dispositivos intermediários, como firewalls e proxies, para amplificar tráfego em campanhas de negação de serviço distribuída (DDoS). Foram conduzidos experimentos em laboratório com firewalls pfSense e FortiGate, avaliando a eficácia da técnica e o comportamento dos dispositivos sob ataque. Adicionalmente, realizou-se varredura no espaço IP brasileiro com a ferramenta ZMap e pacotes TCP personalizados, identificando middleboxes vulneráveis.**

***Termos do Índice*—ataques de reflexão amplificada, middleboxes, DoS, DDoS, negação de serviço, redes, segurança da informação.**

I. Introdução

Nos últimos anos, profissionais de segurança cibernética envolvidos na mitigação e resposta a ataques de negação de serviço (DoS, *Denial of Service*) e ataques distribuídos de negação de serviço (DDoS, *Distributed Denial of Service*) têm enfrentado desafios cada vez mais complexos. Esses desafios decorrem da rápida evolução de técnicas de ataque sofisticadas, incluindo novas formas de DDoS baseadas em reflexão e amplificação [1]. Embora tais ataques sejam tradicionalmente associados ao protocolo UDP [2], estudos recentes mostram que eles também podem ser executados por meio do TCP. Uma forma de exploração desse protocolo foi demonstrada por Bock et al. [3], que evidenciaram que ataques de reflexão e amplificação via TCP podem ocorrer ao explorar comportamentos inadequados de middleboxes, dispositivos intermediários que inspecionam, filtram e modificam pacotes de dados [3] [4].

Middleboxes, como firewalls, proxies e sistemas de prevenção de intrusão (IPS) [5], são amplamente utilizados em redes corporativas. No entanto, quando mal configurados, podem se tornar vetores de ataque. Nesses casos, um atacante envia pacotes TCP com o endereço IP de origem falsificado, correspondente à vítima. A middlebox, ao processar esses pacotes, gera respostas amplificadas diretamente para o alvo, ocultando a verdadeira origem do ataque. Mesmo soluções de segurança avançadas, como os Next Generation Firewalls (NGFWs), podem apresentar vulnerabilidades em algumas versões, permitindo que esses dispositivos atuem como amplificadores. O impacto desse tipo de exploração pode ser severo, resultando em prejuízos financeiros significativos e danos à reputação da organização.

Diversos ataques explorando middleboxes já foram documentados. Em março de 2022, a Akamai identificou campanhas DDoS com picos de até 11 Gbps, confirmando o uso da técnica de reflexão via middlebox [4]. Embora ainda em menor escala que outros vetores de DDoS, a frequência e intensidade desses ataques estão crescendo, indicando que a técnica está se tornando um recurso comum nos arsenais de atacantes [4].

O objetivo deste trabalho é demonstrar e analisar, por meio de experimentos práticos, como os ataques de reflexão amplificada sobre TCP podem ser explorados em middleboxes. Primeiramente, um algoritmo de ataque foi aplicado e avaliado em três ambientes controlados distintos, com o objetivo de analisar o comportamento das middleboxes. Em seguida, o estudo foi expandido por meio de uma varredura em larga escala no espaço IP brasileiro, a fim de identificar a vulnerabilidade de middleboxes em redes reais do país e avaliar sua proporção em um cenário mais amplo.

II. Ataque de reflexão amplificada sobre TCP explorando middleboxes

Um ataque de reflexão amplificada sobre TCP usando middleboxes ocorre quando dispositivos intermediários são manipulados para gerar grandes volumes de tráfego contra uma vítima. Isso explora a implementação incorreta do protocolo TCP, que permite que as middleboxes respondam a pacotes fora de estado sem o handshake completo [6] [7]. Esse ataque possui uma taxa de amplificação significativa, conforme a Equação 1.

$$\text{Taxa de Amplificação} = \frac{\text{Dados recebidos pela vítima}}{\text{Dados enviados pelo atacante}} \quad (1)$$

Nesse tipo de ataque, o invasor envia pacotes TCP forjados, nos quais insere o endereço IP da vítima como origem. Esses

pacotes contêm requisições HTTP direcionadas a domínios considerados proibidos, como sites de pornografia, armamentos ou outros conteúdos bloqueados. A middlebox, ao realizar a inspeção, interpreta o tráfego como legítimo e aplica suas regras de bloqueio ou filtragem, gerando respostas automáticas que são encaminhadas diretamente ao endereço da vítima, incluindo respostas como páginas de bloqueio (com conteúdo HTML, imagens ou scripts), cabeçalhos HTTP ou pacotes TCP com dados extras. Como essas respostas podem ser maiores que a requisição inicial, ocorre um efeito de amplificação, resultando em um volume elevado de tráfego malicioso direcionado ao alvo [3], [4].

O ataque foi descrito pela primeira vez por Kevin Bock e sua equipe de pesquisadores da Universidade de Maryland e da Universidade do Colorado em Boulder, no artigo científico "Weaponizing Middleboxes for TCP Reflected Amplification" [3]. No estudo, os autores realizaram uma varredura em toda a internet IPv4 para identificar middleboxes vulneráveis, constatando que muitas delas oferecem fatores de amplificação superiores a 100 vezes. Além disso, observaram que esse tipo de ataque ocorre principalmente em ambientes associados a regimes de censura, onde tais dispositivos são amplamente utilizados para inspeção e bloqueio de tráfego.

A defesa contra esse tipo de ataque é dificultada pelo uso de portas comuns (como TCP 80) e pelo fato de os pacotes conterem requisições HTTP válidas, o que inviabiliza a detecção baseada em assinatura. Dessa forma, a mitigação exige modificações no comportamento padrão das middleboxes, bem como atualizações de firmware para reduzir a superfície de exploração [6].

III. Estratégias de mitigação ao ataque de reflexão amplificada sobre TCP explorando middleboxes

Os ataques de reflexão amplificada sobre TCP que exploram middleboxes representam um problema complexo que afeta diversas implementações e dispositivos de rede, não havendo solução única aplicável a todos os contextos [3]. Uma das principais estratégias consiste em exigir que o middlebox observe ambas as direções da comunicação e valide o estabelecimento completo do handshake TCP antes de injetar qualquer resposta, prevenindo respostas a pacotes forjados [3].

Pacotes SYN com payload são indicativos de tráfego malicioso, pois em contextos legítimos raramente contêm dados [4]. Recomenda-se bloquear esses pacotes e descartar conexões com payloads vindos das portas 80 ou 443. Exemplo de regra de ACL prática:

```
deny tcp any eq 80 host x.x.x.x match-all +SYN -ack
    packet-length gt 100
```

Outra abordagem é limitar o tamanho das respostas emitidas por middleboxes, utilizando pacotes RST simples, redirecionamentos HTTP mínimos ou páginas de bloqueio simples, reduzindo o fator de amplificação [3], [8]. A simplificação de páginas de bloqueio e a restrição de respostas a tráfego interno e regiões específicas também são recomendadas.

Recomenda-se ainda desabilitar respostas HTTP desnecessárias, priorizando HTTPS seguro, e enviar pacotes RST quando o IP de origem não responde, encerrando sessões indefinidas [9]. A técnica de reflexão TCP-middlebox explora pacotes SYN com payload e solicitações em múltiplas portas, tornando varreduras tradicionais ineficazes [10]. Isso reforça a necessidade de estratégias de mitigação proativas e integradas, que combinem validação completa do handshake, limitação de respostas e respostas simples a requisições suspeitas.

IV. Metodologia do uso do código e do ambiente de laboratório

O código utilizado para a realização dos ataques foi obtido de um repositório público no GitHub, de autoria do usuário `moloch54`, intitulado "Ddos-TCP-Middlebox-Reflection-Attack" [11]. O projeto inclui o arquivo `mra.py`, responsável pela execução dos ataques. Após investigação, verificou-se que o autor do código é Sébastien Meniere, residente em Nancy, França. Em contato direto, obtivemos autorização para o uso do código e a confirmação de que ele ainda não havia sido testado em ambiente laboratorial, reforçando a relevância dos experimentos conduzidos.

A escolha desse código se deveu à sua aderência à metodologia de Bock et al. [3], o que garantiu conformidade com o ataque e maior precisão nos resultados. A utilização de uma ferramenta já consolidada permitiu concentrar os esforços na análise experimental, evitando riscos de inconsistências decorrentes do desenvolvimento de uma nova implementação.

O ambiente de laboratório contemplou três cenários, baseados na mesma topologia (Figura 1), compostos por três elementos: um alvo, um atacante e uma middlebox (firewall). No primeiro cenário, utilizou-se pfSense com pfBlockerNG; no segundo, pfSense com Squid e SquidGuard; e, no terceiro, FortiGate. Em todos os cenários, os domínios `youporn.com` (66.254.114.79), `facebook.com` (157.240.13.35), `pornhub.com` (66.254.114.41) e `bittorrent.com` (98.143.146.7) foram configurados como proibidos, correspondendo aos utilizados pelo código de ataque.

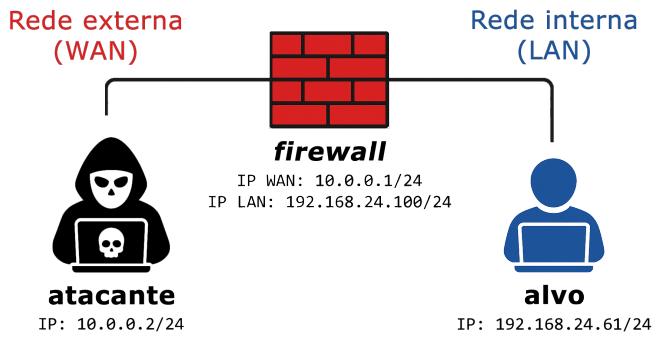

Fig. 1: Topologia da rede do laboratório utilizada nos três cenários experimentais do ataque.

Os firewalls foram deliberadamente configurados para simular tanto ambientes corporativos típicos quanto configurações incorretas, de modo a evidenciar como certas escolhas podem

expor esses dispositivos a ataques de reflexão amplificada sobre TCP, mesmo tratando-se de soluções amplamente utilizadas.

Além disso, a configuração completa do ambiente experimental empregado na análise dos ataques de reflexão amplificada sobre TCP, incluindo documentação do código-fonte, elementos virtuais, topologia de rede e configurações do laboratório, encontra-se detalhadamente registrada em repositório público disponível em: https://github.com/paulovictorbrines/TCP_Middlebox_Reflection_Attack_Lab.

A. Resultados do firewall pfSense + pfBlockerNG

Nos testes realizados com o pfSense em conjunto com o pfBlockerNG, ferramenta responsável pelo bloqueio baseado em domínios e listas de IP, exibindo ao usuário uma página de bloqueio, verificou-se que o sistema apenas redireciona as solicitações destinadas a domínios proibidos para a página local de bloqueio do próprio pfBlockerNG. Esse comportamento caracteriza-se apenas como reflexão, uma vez que não há envio de conteúdo HTML externo. Assim, a taxa de amplificação resultante é igual a 1,00x, conforme definido na Equação 1. O registro dessa reflexão foi identificado nos logs do pfSense, conforme ilustrado na Figura 3.

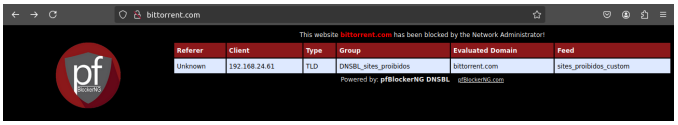

Fig. 2: Página de bloqueio do pacote pfBlockerNG no pfSense.

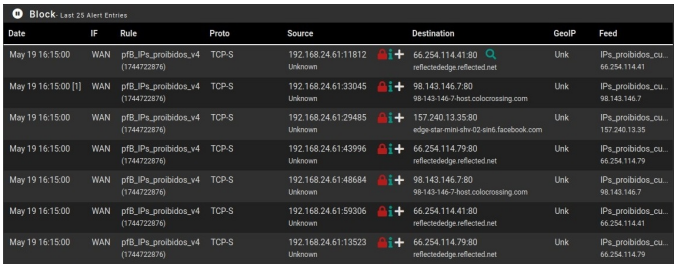

Fig. 3: Logs do pfBlockerNG no pfSense, evidenciando o bloqueio bem-sucedido de domínios classificados como proibidos durante a execução do ataque.

B. Resultados do firewall pfSense + Squid + SquidGuard

Como alternativa ao primeiro cenário (IV-A) e com o objetivo de avaliar a possibilidade de amplificação do tráfego, foi utilizada a combinação do firewall pfSense com o Squid (proxy) e o SquidGuard (filtro de conteúdo). Diferentemente do pfBlockerNG, que apenas redireciona domínios proibidos, o SquidGuard envia efetivamente uma página HTML de bloqueio ao usuário, como mostrado na Figura 4. Essa diferença motivou a escolha desta configuração para o segundo cenário experimental.

Durante os testes de acesso manual a domínios proibidos via navegador, o bloqueio foi aplicado corretamente. Contudo,

Fig. 4: Página de bloqueio do pacote SquidGuard no pfSense.

em cenários de ataque com pacotes forjados, o tráfego é liberado sem qualquer interceptação ou resposta. Essa falha ocorre porque, aparentemente, o SquidGuard não inspeciona pacotes que não façam parte do processo de handshake TCP, permitindo assim a passagem de tráfego.

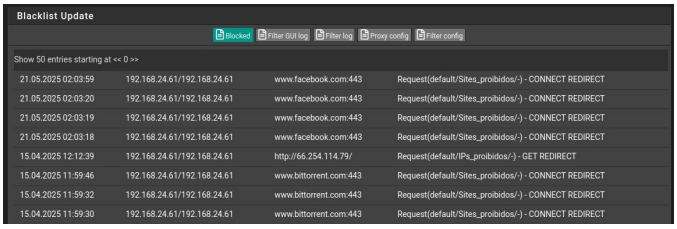

Fig. 5: Logs do SquidGuard, integrado ao Squid no pfSense, evidenciando o bloqueio bem-sucedido de domínios classificados como proibidos durante acesso manual via navegador.

C. Resultados do firewall FortiGate

Para contornar as limitações observadas nos dois primeiros cenários (IV-A e IV-B), foi utilizado o firewall FortiGate. Esta escolha se justifica por ser uma alternativa mais robusta e pela versão utilizada (7.2.0) ser vulnerável ao ataque conforme a CVE-2022-27491 [12] [13] [14]. Diferentemente do pfBlockerNG e semelhante ao Squid em conjunto com o SquidGuard, o FortiGate envia uma página HTML de bloqueio ao usuário (Figura 6) e é amplamente utilizado em instituições corporativas e governamentais.

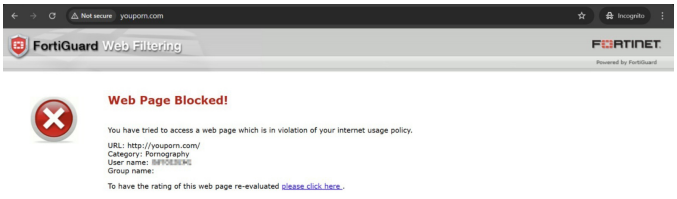

Fig. 6: Página de bloqueio do FortiGate.

O comportamento observado foi similar ao do primeiro cenário (IV-A), gerando reflexão, mas sem amplificação, como evidenciado nos logs da Figura 7, resultando em uma taxa de amplificação de 0,68x, conforme a Equação 1. O FortiGate possui comportamento mais rigoroso na verificação do estado TCP e exige o estabelecimento completo da conexão (three-way handshake) para exibir a página de bloqueio, o que reduz o número de pacotes refletidos devido à verificação rigorosa do estado TCP.

Date/Time	Source	Device	Destination	Application Name	Result	Policy ID
46 minutes ago	192.168.24.61		157.240.13.35		Deny: UTM Blocked	WAN -> INTERNET (3)
46 minutes ago	192.168.24.61		66.254.114.41		Deny: UTM Blocked	WAN -> INTERNET (3)
46 minutes ago	192.168.24.61		98.143.146.7		Deny: UTM Blocked	WAN -> INTERNET (3)
46 minutes ago	192.168.24.61		98.143.146.7		Deny: UTM Blocked	WAN -> INTERNET (3)
46 minutes ago	192.168.24.61		157.240.13.35		Deny: UTM Blocked	WAN -> INTERNET (3)
46 minutes ago	192.168.24.61		98.143.146.7		Deny: UTM Blocked	WAN -> INTERNET (3)
46 minutes ago	192.168.24.61		66.254.114.41		Deny: UTM Blocked	WAN -> INTERNET (3)
46 minutes ago	192.168.24.61		66.254.114.79		Deny: UTM Blocked	WAN -> INTERNET (3)
46 minutes ago	192.168.24.61		66.254.114.41		Deny: UTM Blocked	WAN -> INTERNET (3)

Fig. 7: Logs do FortiGate evidenciando o bloqueio bem-sucedido de domínios classificados como proibidos durante a execução do ataque.

D. Comparativo dos resultados dos três firewalls

Na Figura 8, observa-se o envio dos pacotes forjados pelo atacante nos cenários IV-A e IV-C, com endereços IP de origem falsificados (correspondentes à vítima) e contendo flags `SYN`, simulando uma comunicação legítima com serviços potencialmente bloqueados por middleboxes. Esses pacotes acionam as middleboxes a gerar respostas refletidas.

A Figura 9 apresenta o efeito direto dessa manipulação: pacotes enviados pelas middleboxes em resposta às requisições forjadas, recebidos pelo host da vítima. Esses pacotes constituem o tráfego refletido, evidenciando a exploração prática de middleboxes como vetores de ataque.

A Tabela I sintetiza os resultados, indicando o volume de pacotes enviados pelo atacante, o volume de pacotes refletidos e recebidos pelo alvo, a porcentagem recebida em relação ao total enviado e a taxa de amplificação para cada middlebox testada. Os resultados do Squid com SquidGuard foram excluídos devido à ausência de dados representativos: embora o bloqueio via navegador tenha ocorrido, o tráfego gerado pelo código de ataque foi permitido, evidenciando comportamento inconsistente do proxy diante de diferentes tipos de requisição.

Nos demais cenários, o pfSense com pfBlockerNG refletiu praticamente todos os pacotes (quase 100%), com amplificação unitária (1,00x). O FortiGate apresentou uma taxa de reflexão de aproximadamente 67,7%, resultando em amplificação inferior a 1 (0,68x). Esses resultados demonstram que, mesmo sem injeção significativa de conteúdo, ou seja, sem amplificação, houve reflexão da middlebox para o alvo, confirmando a eficácia da técnica.

No.	Time	Source	Destination	Protocol	Length	Info
17	0.001815	192.168.24.61	66.254.114.41	TCP	54	30544 → 80 [SYN] Seq=0 Win=8192 Len=0
18	0.001905	192.168.24.61	98.143.146.7	TCP	54	45783 → 80 [SYN] Seq=0 Win=8192 Len=0
19	0.002032	192.168.24.61	66.254.114.79	TCP	54	8618 → 80 [SYN] Seq=0 Win=8192 Len=0
20	0.002120	192.168.24.61	157.240.13.35	TCP	54	42221 → 80 [SYN] Seq=0 Win=8192 Len=0
21	0.002247	192.168.24.61	157.240.13.35	TCP	54	24639 → 80 [SYN] Seq=0 Win=8192 Len=0
22	0.002336	192.168.24.61	98.143.146.7	TCP	54	38563 → 80 [SYN] Seq=0 Win=8192 Len=0
23	0.002474	192.168.24.61	157.240.13.35	TCP	54	5355 → 80 [SYN] Seq=0 Win=8192 Len=0
24	0.002562	192.168.24.61	98.143.146.7	TCP	54	42691 → 80 [SYN] Seq=0 Win=8192 Len=0
25	0.002673	192.168.24.61	98.143.146.7	TCP	54	12898 → 80 [SYN] Seq=0 Win=8192 Len=0
26	0.002763	192.168.24.61	66.254.114.41	TCP	54	45431 → 80 [SYN] Seq=0 Win=8192 Len=0
27	0.002892	192.168.24.61	66.254.114.79	TCP	54	17521 → 80 [SYN] Seq=0 Win=8192 Len=0
28	0.002980	192.168.24.61	66.254.114.41	TCP	54	31791 → 80 [SYN] Seq=0 Win=8192 Len=0

Fig. 8: Trecho da captura de pacotes `atacante.pcap` no Wireshark, mostrando os pacotes forjados enviados pelo atacante com o objetivo de iniciar o ataque de reflexão TCP.

V. Metodologia da varredura no espaço IPv4 do Brasil

Este estudo utilizou uma metodologia inspirada em testes realizados por organizações como a ShadowServer [10] (https://www.shadowserver.org/news/over-18-8-million-ips-vulnerable-to-middlebox-tcp-reflection-ddos-attacks) e a Akamai [4]

No.	Time	Source	Destination	Protocol	Length	Info
17	9.890023	157.240.13.35	192.168.24.61	TCP	60	80 → 5014 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
18	9.890189	157.240.13.35	192.168.24.61	TCP	60	80 → 50629 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
19	9.890749	66.254.114.79	192.168.24.61	TCP	60	80 → 8618 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
20	9.890983	98.143.146.7	192.168.24.61	TCP	60	80 → 49538 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
21	9.891132	66.254.114.41	192.168.24.61	TCP	60	80 → 46733 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	9.891284	98.143.146.7	192.168.24.61	TCP	60	80 → 3933 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	9.891425	98.143.146.7	192.168.24.61	TCP	60	80 → 25510 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	9.891568	66.254.114.41	192.168.24.61	TCP	60	80 → 30544 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
25	9.891722	98.143.146.7	192.168.24.61	TCP	60	80 → 45783 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
26	9.891897	157.240.13.35	192.168.24.61	TCP	60	80 → 42221 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	9.892956	157.240.13.35	192.168.24.61	TCP	60	80 → 24639 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
28	9.892957	157.240.13.35	192.168.24.61	TCP	60	80 → 5355 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Fig. 9: Trecho da captura de pacotes `alvo.pcap` no Wireshark, mostrando as respostas enviadas pelo firewall ao host alvo como resultado do ataque de reflexão TCP durante o ataque

(https://www.akamai.com/blog/security/tcp-middlebox-reflection). Além disso, buscou-se validar e aprofundar os resultados apresentados por Bock et al. [3].

O objetivo principal foi escanear o espaço de endereçamento IPv4 brasileiro para identificar middleboxes vulneráveis capazes de refletir respostas HTTP a partir de pacotes SYN malformados. A motivação foi avaliar a presença e a distribuição de vulnerabilidades, bem como o potencial de exploração no território brasileiro, considerando respostas esperadas como SYN-ACK, RST com payloads ou páginas de bloqueio, entre outras.

A. Ferramentas e Execução da Varredura

A varredura foi realizada utilizando uma versão customizada do ZMap, um scanner de rede rápido e modular projetado para pesquisas em larga escala. Esta versão incorporou o módulo `forbidden_scan`, desenvolvido por Bock et al. [3], que não faz parte do ZMap oficial. O módulo envia pacotes TCP SYN com payload HTTP, um padrão atípico que visa provocar respostas de middleboxes que inspecionam pacotes antes da conclusão do handshake TCP. O código do módulo está disponível em: https://github.com/Kkevsterrr/zmap/blob/master/src/probe_modules/module_forbidden_scan.c.

A lista de endereços IPv4 brasileiros foi obtida no formato CIDR (ex.: 138.97.188.0/22) a partir do site Country IP Blocks (https://www.countryipblocks.net/acl.php). A varredura foi executada com o seguinte comando, após a clonagem e compilação do repositório do ZMap modificado:

```
sudo src/zmap -i ens37 -M forbidden_scan -p 80 \
-w "blocos_ipv4_brasil.txt" \
-f "saddr,len,payloadlen,flags,validation_type" \
-o "scan/scan_brasil.csv" -O csv
```

O comando escaneou a porta 80, registrando no arquivo `scan_brasil.csv` o endereço de origem (`saddr`), o comprimento do payload (`payloadlen`) e as flags TCP (`flags`) das respostas, informações essenciais para a análise de reflexão e amplificação de tráfego.

B. Análise Estatística e Geração de Gráficos

Os dados brutos da varredura, armazenados em formato CSV (`scan_brasil.csv`), foram processados por um script Python chamado `stats.py` (https://github.com/breakerspace/weaponizing-censors). O script analisou as respostas recebidas, extraindo estatísticas relevantes para avaliar o potencial de reflexão e amplificação das middleboxes.

O script foi executado com o comando:

TABELA I: Comparativo dos resultados obtidos durante cinco minutos de ataque nas middleboxes pfSense + pfBlockerNG e FortiGate

Middlebox	Pacotes enviados	Pacotes recebidos	% recebido	Amplificação
pfSense + pfBlockerNG	2.044.369	2.044.368	99,99%	1.00x
FortiGate	2.044.328	1.384.473	67,73%	0.68x

```
sudo python3 stats.py zmap/scan/scan_brasil.csv 149
```

O parâmetro `149` corresponde ao tamanho do pacote de sonda enviado. O script calculou métricas como o número de IPs que geraram amplificação, a taxa média de amplificação observada e a distribuição das flags TCP nas respostas.

VI. Resultados da Varredura

Para contornar restrições impostas por provedores de internet, a varredura inicial no espaço IPv4 brasileiro foi realizada por meio de uma VPN com saída nos EUA. Essa abordagem permitiu identificar 13.299.793 IPs únicos que responderam às requisições, a partir de um total de 40.805.661 blocos. A varredura, conduzida com ZMap e o módulo `forbidden_scan`, durou aproximadamente 2 horas e 26 minutos e foi concluída com sucesso. Desses IPs respondentes, 4.541.741 (aproximadamente 34%) foram classificados como amplificadores, indicando vulnerabilidade a ataques de reflexão amplificada via TCP (Tabela II).

O elevado número de IPs amplificadores não corresponde ao número real de middleboxes distintas, pois muitos IPs respondem por trás de poucas middleboxes. Essa concentração confirma a presença de middleboxes vulneráveis distribuídas pelo espaço brasileiro. As Figuras 11 e 12 ilustram, respectivamente, o quantitativo e a proporção de IPs classificados como amplificadores. A Figura 10 apresenta a distribuição das flags TCP nos pacotes de resposta, fornecendo informações sobre o comportamento dos sistemas de rede dos respondentes.

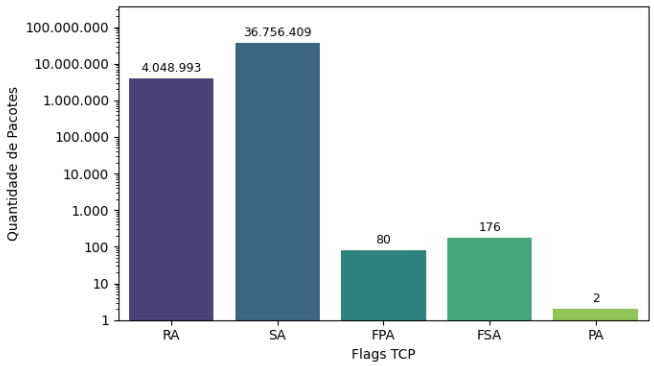

Fig. 10: Distribuição das flags TCP nos pacotes de resposta emitidos pelos IPs.

Na análise detalhada, a predominância da flag **SYN-ACK** (36.756.409 pacotes) evidencia um comportamento que favorece ataques de amplificação, mesmo sem estabelecimento completo de handshake. O comportamento dos amplificadores foi analisado por meio de Funções de Distribuição Acumulada (CDFs), apresentadas nas Figuras 13, 14 e 15, que mostram, respectivamente, a distribuição de pacotes, bytes e taxas de amplificação por IP. Esses resultados demonstram que a amplificação TCP é viável em larga escala, mesmo em cenários sem conexão completa.

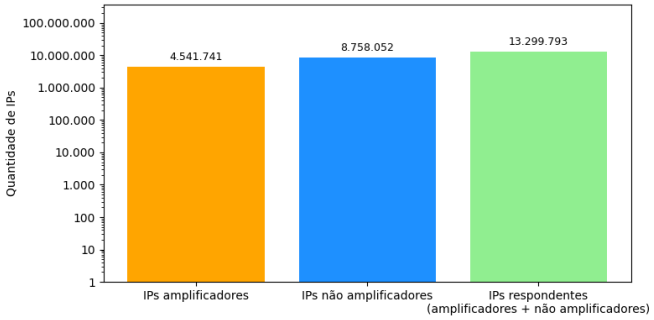

Fig. 11: Quantitativo de endereços IP que responderam à varredura em amplificadores e não amplificadores, incluindo o total de respondentes.

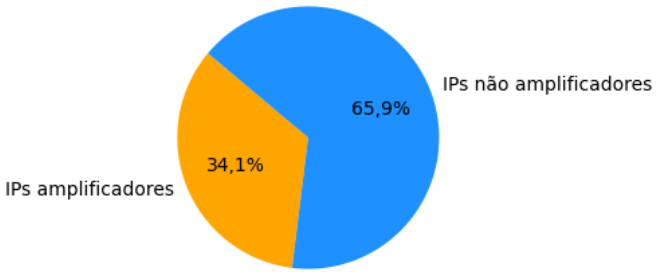

Fig. 12: Percentual de IPs respondentes classificados como amplificadores e não amplificadores.

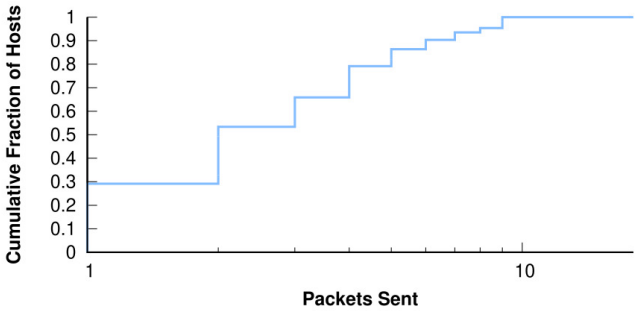

Fig. 13: Distribuição acumulada da fração de hosts amplificadores em função do número de pacotes enviados por cada IP.

VII. Conclusões

Este trabalho demonstrou que o ataque de reflexão amplificada via middleboxes constitui uma ameaça real e viável,

TABELA II: Resultados das varreduras em diferentes blocos de endereço IP.

Rede	IPs respondentes	IPs amplificadores	IPs não amplificadores	Bytes amplificados	Amplificação média
Brasil	13.299.793	4.541.741	8.758.052	1.119.928.020	1,655x
A	12.481	8.819	3.662	2.334.588	1,777x
B	6.319	4.444	1.875	1.173.560	1,772x

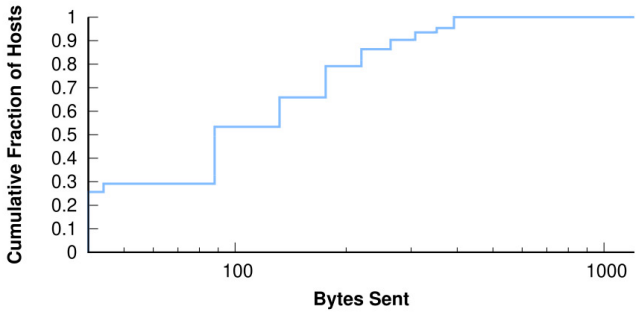

Fig. 14: Distribuição acumulada da fração de hosts amplificadores em função do número de bytes enviados por cada IP.

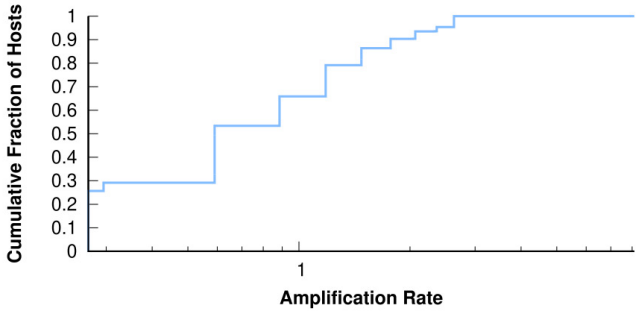

Fig. 15: Distribuição acumulada da fração de hosts em função da taxa de amplificação observada em cada IP amplificador.

demandando atenção de profissionais e pesquisadores. Para isso, realizou-se um estudo detalhado do tema, envolvendo o desenvolvimento de um ambiente de laboratório para testes controlados e uma varredura em larga escala no espaço IPv4 brasileiro.

No ambiente de laboratório, mesmo sem grandes volumes de amplificação, a reflexão de pacotes para o alvo comprovou a viabilidade do ataque em cenário controlado. Este foi o primeiro registro de aplicação bem-sucedida do código de teste em um ambiente real, validando o conceito do ataque.

A varredura nacional revelou um número de IPs vulneráveis muito superior ao esperado. Milhões de IPs responderam aos pacotes de sondagem, evidenciando a presença de diversas middleboxes suscetíveis à amplificação de tráfego. Esses resultados confirmam a relevância e a gravidade do problema, ressaltando a necessidade de conscientização sobre esse vetor de ataque em infraestruturas de rede.

Referências

[1] E. J. A. Silva, G. R. L. Andrade, and R. L. S. Oliveira, "Ataques Negação de Serviço Distribuído (DDoS): o Que é e Como Prevenir," 2024.

[2] Nexusguard, "DDoS Trend Report 2024," 2024. [Online]. Available: https://www.nexusguard.com/threat-report/ddos-trend-report-2024

[3] K. Bock, A. Alaraj, Y. Fax, K. Hurley, E. Wustrow, and D. Levin, "Weaponizing Middleboxes for TCP Reflected Amplification: Censors pose a threat to the entire Internet." Aug. 2021. [Online]. Available: https://geneva.cs.umd.edu/posts/usenix21-weaponizing-censors/

[4] Akamai Security Intelligence Response Team, "TCP Middlebox Reflection: Coming to a DDoS Near You," Mar. 2022. [Online]. Available: https://www.akamai.com/blog/security/tcp-middlebox-reflection

[5] S. Huang, F. Cuadrado, and S. Uhlig, "Middleboxes in the Internet: A HTTP perspective," *2017 Network Traffic Measurement and Analysis Conference (TMA)*, pp. 1–9, 2017.

[6] K. Bock, A. Alaraj, Y. Fax, K. Hurley, E. Wustrow, and D. Levin, "Weaponizing Middleboxes for TCP Reflected Amplification," *30th USENIX Security Symposium (USENIX Security 21)*, pp. 3345–3361, Aug. 2021. [Online]. Available: https://www.usenix.org/conference/usenixsecurity21/presentation/bock

[7] D. Pal, "A new DDoS attack vector: TCP Middlebox Reflection," Oct. 2022. [Online]. Available: https://blog.apnic.net/2022/10/18/a-new-ddos-attack-vector-tcp-middlebox-reflection/

[8] INCIBE, "TCP Middlebox Reflection: new DDoS attack vector," May 2022. [Online]. Available: https://www.incibe.es/en/incibe-cert/blog/tcp-middlebox-reflection-new-ddos-attack-vector

[9] J. Ji, "7 Gbps TCP-Middlebox-Reflection Incident Mitigated by NSFOCUS - NSFOCUS, Inc., a global network and cyber security leader, protects enterprises and carriers from advanced cyber attacks." Apr. 2022. [Online]. Available: https://nsfocusglobal.com/pt-br/7-gbps-tcp-middlebox-reflection-incident-mitigated-by-nsfocus/

[10] Shadowserver Foundation, "Over 18.8 million IPs vulnerable to Middlebox TCP reflection DDoS attacks," Apr. 2022. [Online]. Available: https://www.shadowserver.org/news/over-18-8-million-ips-vulnerable-to-middlebox-tcp-reflection-ddos-attacks/

[11] S. Meniere, "Ddos-TCP-Middlebox-Reflection-Attack," 2023. [Online]. Available: https://github.com/moloch54/Ddos-TCP-Middlebox-Reflection-Attack

[12] NIST, "CVE-2022-27491," Sep. 2022. [Online]. Available: https://nvd.nist.gov/vuln/detail/cve-2022-27491

[13] SecAlerts, "CVE-2022-2749: TCP Middlebox Reflection," Sep. 2022. [Online]. Available: https://secalerts.co/vulnerability/CVE-2022-27491

[14] FortiGuard Labs, "TCP Middlebox Reflection," Sep. 2022. [Online]. Available: https://www.fortiguard.com/psirt/FG-IR-22-073