Compilação de artigos com análise comparativa de ataques cibernéticos em redes IPv4 e IPv6

Artigos	Autores	Critério de Mitigação	Resultado em Rede IPv4	Resultado em Rede IPv6
Controlled ddos attack on ipv4/ipv6 network using distributed computing infrastructureontrolled ddos attack on ipv4/ipv6 network using distributed computing infrastructure	ČERŇANSKÝ, Michal; HURAJ, Ladislav; ŠIMON, Marek	Cookies SYN para mitigação de ataques SYN flood	Eficaz contra SYN flood; vulnerável a HTTP GET flood (carga CPU=16, memória=23%, indisponível após 19s) e SMTP flood (carga CPU>10, memória=17%)	Eficaz contra SYN flood; vulnerável a HTTP GET flood (carga CPU=14, memória=27%, indisponível após 29s) e SMTP flood (carga CPU=8, memória=14%)
Ipv6 network ddos attack with p2p gridpv6 network ddos attack with p2p grid	ŠIMON, Marek; HURAJ, Ladislav; HOSŸOVECKÝ, Marián	Ambiente de teste controlado P2P (OurGrid) para análise e desenvolvimento de contramedidas	Maior carga de CPU no sistema alvo durante HTTP GET flood	Menor carga de CPU (devido a cabeçalho mais simples), ~4% mais dados transferidos, vulnerabilidade similar ao IPv4
Deep learning approach for detecting icmpv6 flood ddos attacks in ipv6 networkseep learning approach for detecting icmpv6 flood ddos attacks in ipv6 networks	ELEJLA, Omar E.; HASBULLAH, Iznan H.; ANBAR, Mohammed; BAHASHWAN, Abdullah Ahmed; HAMOUDA, Shady; FAISAL, Serri	LSTM com seleção de características (IGR + qui-quadrado) para detecção em tempo real	Não aplicável - método desenvolvido especificamente para IPv6	Precisão 98,41%, FPR 0,551%, medida F 98,39%, supera modelos RNN (92,3%) e GRU (98,31%)
Performance evaluations of iptables firewall solutions for ddos attackserformance evaluations of iptables firewall solutions for ddos attacks	ŠIMON, Marek; HURAJ, Ladislav; ŸERŸANSKÝ, Michal	IPTables/IP6Tables com regras específicas anti-HTTP GET flood e limitação de conexões	Eficaz na mitigação, mas com maior consumo de CPU	Eficaz na mitigação, 21,8% menor carga CPU, 0,769s melhor tempo de resposta que IPv4
Detection and mitigation of flood attacks in ipv6-enabled software defined networksetection and mitigation of flood attacks in ipv6-enabled software defined networks	ASHIMI, Quadri OLUWATOBI; ADENIJI, Oluwashola David	Limiar dinâmico em SDN com monitoramento sFlow e regras OpenFlow para bloqueio automático	Tempo de mitigação de 66,6%, detecção e resposta em 4s cada	Tempo de mitigação de 46,6% (melhor desempenho), detecção e resposta em 4s cada
Configuring hosts for automatic network connectivity detection	HAMARSHEH, Ala; GOOSSENS, Marnix;	Não apresenta critério de mitigação DDoS (foco	Performance de referência - throughput 14,98-74,34 Mbps,	Performance próxima ao IPv4 nativo (14,83-74,46 Mbps),

(ipv6, ipv6 over ipv4 or ipv4)onfiguring hosts for automatic network connectivity detection (ipv6, ipv6 over ipv4 or ipv4)	ALSERHAN, Rafe Alasem	em protocolo CHANC para conectividade)	usado como baseline	CHANC alcança 14,87-74,27 Mbps
Nat64 performance evaluationat64 performance evaluation	POKORNÝ, Jan; GRÉGR, Ing. Matěj; (SUPERVISOR), Ph.D.	Não apresenta critério de mitigação DDoS (foco em avaliação de desempenho NAT64)	Throughput ~10 Gbps (roteamento puro e NAT44), performance máxima teórica	Throughput ~10 Gbps (com Jool otimizado), equivalente ao IPv4 após otimizações
Ddos attacks and defense mechanisms: classification and state-of-the-artdos attacks and defense mechanisms: classification and state-of-the-art	DOULIGERIS, Christos; MITROKOTSA, Aikaterini	Tolerância à falhas, QoS (IntServ/DiffServ), Class-based Queuing (CBQ), arquitetura Pushback	Discussão teórica de mecanismos - filtragem de ingressos/egressos, uso de TOS, controle de broadcast	Não apresenta resultados ou análises específicas para IPv6
A new approach to detect, filter and track ddos attack new approach to detect, filter and track ddos attack	GOMATHI, S.; KARTHIKEYAN, Dr. E.	Combinação de Filtro de Contagem de Saltos Atualizado (UHCF) + Algoritmo de Marcação Probabilística de Pacotes Eficiente (EPPM)	Não especificado - método apresentado de forma geral	Não especificado - método apresentado de forma geral
Detection and defense mechanisms against ddos attacks using ip address spoofingetection and defense mechanisms against ddos attacks using ip address spoofing	PIMPALKAR, Archana S.; PATIL, AR Bhagat	Autenticação criptográfica com HMAC usando chave secreta baseada em campos do cabeçalho IP	99,9% de precisão, 0% falsos positivos, filtrou 2.289 pacotes de ataque em 20ms sem afetar 1.130 pacotes legítimos	Não aplicável - método desenvolvido especificamente para IPv4
Network protection against ddos attacksetwork protection against ddos attacks	DZURENDA, Petr; MARTINASEK, Zdenek; MALINA, Lukas	DefensePro 6.10.00 com estratégia de 4 etapas (prevenção, detecção, reação, manutenção do tráfego legítimo)	100% de disponibilidade durante ataques, suporta até 900 Mbps de intensidade de ataque (18x maior que ataques típicos)	Não testado - experimentos realizados apenas em IPv4