Manual da Solução Anti-DDoS Huge Networks

Proteção inovadora para o seu negócio

- HugeGuard Cloud
- HugeGuard Wall
- HugeGuard Hybrid

A continuidade dos seus serviços online é crítica para o seu negócio. A solução Anti-DDoS da Huge Networks foi desenvolvida para oferecer uma blindagem robusta e inteligente, mantendo sua operação **sempre ativa e protegida** contra as mais sofisticadas ameaças de negação de serviço distribuído (DDoS).

IPv4 / IPv6	SOC 24/7	≤ 30 s	Brasil
Cobertura total de endereçamento	Operação no Brasil, suporte em português	Mitigação automática inline	Soberania de dados na mitigação

01 Visão Geral

Nossa solução Anti-DDoS assegura a ininterrupta operação dos seus serviços de Internet, eliminando os riscos de saturação de banda e as paralisações causadas por ataques DDoS. Com uma arquitetura avançada, detectamos e mitigamos ataques direcionados a qualquer endereço IP da sua infraestrutura, seja IPv4 ou IPv6, proporcionando uma cobertura completa.

O processo de mitigação é ágil e eficiente, desviando o tráfego suspeito em tempo real através de um sistema de roteamento inteligente. Nossos Centros de Mitigação inspecionam e tratam o tráfego, bloqueando o que é malicioso e garantindo que apenas o tráfego legítimo chegue aos seus destinos finais. A Huge recebe a totalidade do tráfego originado na internet destinado ao cliente, realiza a inspeção e limpeza integralmente usando sua infraestrutura (Centros de Mitigação), sem consumir recursos nem degradar o desempenho da rede do cliente. Tudo isso com a flexibilidade de operação manual ou automática, adaptando-se perfeitamente às suas necessidades.

Priorizamos a soberania dos seus dados: o tráfego para análise e limpeza permanece em território brasileiro. Apenas em casos de tráfego com origem internacional, e se o recurso estiver disponível, ele poderá ser redirecionado para um centro de mitigação no exterior, mantendo sempre a máxima segurança e conformidade.

02 Detecção e Inteligência

Nossa solução vai além da mitigação reativa, oferecendo um sistema de inteligência e controle rigoroso que antecipa e neutraliza ameaças antes que elas causem impacto.

2.1. Inteligência e Análise Preditiva

Sempre um Passo à Frente

- **Reputação de IPs de Ponta:** Criamos e analisamos a reputação de endereços IP com base em informações exclusivas, geradas durante a filtragem de ataques e interligadas aos principais centros mundiais de avaliação de reputação. Isso significa que estamos sempre atualizados sobre as ameaças globais.
- **Integração com Threat Intelligence:** Nossas capacidades são aprimoradas pela integração contínua com sistemas de threat intelligence, garantindo que suas defesas estejam sempre à frente das últimas táticas de ataque.
- **Atualização Constante de Assinaturas:** Mantenha-se protegido contra ameaças emergentes com nosso serviço de atualização constante de assinaturas de ataques, assegurando a eficácia da sua solução durante todo o período de serviço.
- **Mecanismos de Aprendizado Avançados:** Através da análise de anomalias estatísticas e desequilíbrios de volume de tráfego, com perfis (baseline) de curto e longo prazo, nossa solução aprende e se adapta, identificando e respondendo a ataques volumétricos com precisão.
- **Proteção Contra Flash Crowd:** Distinguimos o tráfego legítimo do malicioso em eventos de Flash Crowd, bloqueando exclusivamente o tráfego de ataque e garantindo que seus usuários legítimos não sejam afetados.
- **Coleta Passiva e Não Intrusiva:** Toda a análise é realizada na infraestrutura da Huge Networks, sem instalação de agentes ou utilização de elementos da rede do cliente para coleta de dados.

2.2. Técnicas e Regras de Mitigação

Defesas Multifacetadas para sua tranquilidade

Nossa solução emprega uma gama completa de técnicas e contramedidas para uma proteção abrangente:

- **Listas Brancas (White lists):** Permita apenas o tráfego de origens confiáveis e pré-definidas, garantindo acesso exclusivo para quem importa.
- **Listas Negras (Black lists):** Bloqueie proativamente o tráfego de fontes maliciosas conhecidas, eliminando riscos antes que cheguem à sua rede.
- **Limitação de Taxa (Rate limiting):** Controle o volume de tráfego por prefixo IP, protocolo ou vetor de ataque prevenindo sobrecargas e mantendo a performance ideal.
- **Desafio-Resposta (Challenge-response):** Diferencie humanos de bots de forma inteligente, barrando ataques automatizados.
- **Descarte Automático de Pacotes:** Elimine pacotes malformados ou suspeitos com base em padrões anômalos, protegendo sua infraestrutura contra vulnerabilidades.
- **Bloqueio Geográfico:** Personalize suas regras de segurança bloqueando IPs por país, adicionando uma camada extra de proteção.
- **Inspeção Profunda de Pacotes (DPI):** Uma análise detalhada para identificar e neutralizar ameaças ocultas.

- **Monitoramento de Tráfego Legítimo em Tempo Real:** Evitamos falsos positivos, garantindo que a proteção não comprometa a experiência dos seus usuários.
- **Técnicas Específicas para HTTP, HTTPS e DNS:** Mitigação especializada para ataques direcionados a esses protocolos, com suporte a diversas camadas do modelo OSI.

Nossa solução permite a aplicação de regras de mitigação com base em parâmetros precisos:

- **Origem IP:** Bloqueie fontes de ataque específicas.
- **Destino IP:** Proteja alvos específicos em sua rede.
- **Combinação Origem + Destino IP:** Defesas personalizadas para cenários complexos.
- **Padrões em payloads:** Para ataques avançados, inclua expressões capazes de bloquear pacotes baseados em padrões no payload.

CENÁRIO EXTREMO

Contingência para Cenários de Saturação Extrema

Mesmo nos cenários mais severos, você não fica desprotegido. Caso o volume de tráfego de um ataque ultrapasse as capacidades de mitigação especificadas ou sature as conexões do AS (Sistema Autônomo) do cliente, nossa equipe aciona contramedidas adicionais de contingência — entre elas, o bloqueio seletivo por blocos de endereços IP de origem no AS pelo qual o ataque esteja ocorrendo. Assim, garantimos uma resposta estruturada até nos eventos que excedem os limites dimensionados, preservando a disponibilidade dos seus serviços.

2.3. Gestão de Listas de Controle de Acesso (ACLs)

Controle total ao seu alcance

Gerencie suas listas negras e brancas com facilidade, através de:

- **Configuração Flexível:** Configure diretamente no equipamento (para serviços on premises) ou aplicação de listas externas (Através do serviço de NOC), adaptando-se ao seu fluxo de trabalho.
- **Inclusão Dinâmica Inteligente:** O tráfego é incluído dinamicamente em listas negras por autenticação de rede ou detecção de limites de tráfego excedidos, garantindo uma resposta automática e eficaz.
- **Prevenção de Bloqueios Indevidos:** Protegemos hosts válidos contra bloqueios por engano, assegurando que suas operações não sejam interrompidas.
- **Remoção Dinâmica de IPs:** Endereços IP bloqueados são automaticamente removidos após um período de tempo seguro, mantendo suas listas sempre otimizadas.

03 Proteção Total para o seu Ecossistema Digital

Nossa solução foi projetada para mitigar ataques que exploram vulnerabilidades em múltiplas Camadas do modelo OSI, protegendo sua infraestrutura IPv4 e IPv6 contra uma vasta gama de ameaças:

3.1. Cobertura de Ameaças Mitigadas

Nenhum vetor de ataque fica de fora

Da camada de enlace à camada de aplicação (camadas 2, 3, 4 e 7 do modelo OSI), nossa solução identifica e neutraliza as principais categorias de ataques conhecidas:

- **Ataques Volumétricos (Bandwidth Flood):** Incluindo UDP Flood e ICMP Flood.
- **Ataques à pilha TCP:** Mau uso de Flags TCP, RST e FIN, SYN Flood, SYN/ACK e TCP Idle Resets.
- **Ataques de Fragmentação:** Proteção contra pacotes IP, TCP e UDP fragmentados.
- **Botnets, Worms e IP Spoofing:** Defesas robustas contra Botnets, Worms e falsificação de endereços IP de origem.
- **Ataques Hit and Run:** A detecção e aplicação de políticas acompanham as variações de tráfego em tempo real, sendo capaz de mitigar ataques efêmeros e de curta duração.
- **Ataques Avançados:** Incluindo ataques que tenham como origem “Command-and-Control”, Point of Sale Malware, Remote Access Trojans (RATs), dentre outros. Com base de dados atualizada diariamente.
- **Ataques à Camada de Aplicação:** Proteção para ataques utilizando protocolos HTTP e DNS volumétricos.

3.2. Soberania de Dados

Sua informação protegida em casa

Mantemos seus dados seguros dentro do território brasileiro durante os procedimentos de mitigação. Apenas o tráfego de origem internacional, se aplicável e com recursos disponíveis, poderá ser redirecionado para um centro de mitigação no exterior, sempre com a máxima segurança e transparência.

SLA DE LATÊNCIA

Desempenho Garantido

Esse compromisso vem acompanhado de desempenho garantido: mesmo nos períodos de ataque, a latência do circuito é de, no máximo, 100 ms (cem milissegundos) quando a mitigação se origina dos nossos centros de limpeza nacionais, e de, no máximo, 250 ms (duzentos e cinquenta milissegundos) quando se origina de centro(s) internacional(is). Soberania de dados e performance, sem que você precise escolher entre uma e outra.

04 Operação, Monitoramento e Relatórios

Nossa proteção vai além da tecnologia: ela é sustentada por uma operação especializada, transparente e sob o seu controle, com compromissos mensuráveis. Conheça a seguir nossa estrutura de suporte 24/7, as ferramentas de monitoramento à sua disposição e os tempos de resposta que garantimos em contrato.

4.1. Centro Operacional de Segurança (SOC) e Suporte

Sua Equipe de Especialistas 24/7

Conte com nosso Centro Operacional de Segurança (SOC) localizado no Brasil, com uma equipe especializada disponível 24 horas por dia, 7 dias por semana.

Oferecemos suporte integralmente em português brasileiro.

Nossa política de mitigação opera, por padrão, em modo automático — mas a escolha é sua: você pode optar, a qualquer momento, pela troca para o modo manual previamente configurado para os ataques detectados, além de alterar o tipo e o alvo de mitigação, com autorização ou manutenção automática. Em qualquer dos modos, automático ou manual, a detecção e a mitigação ocorrem em tempo real (inline). Sem limitações na quantidade de mitigação de ataques ou no volume de tráfego bloqueado, sua proteção é ilimitada.

4.2. Portal de Monitoramento e Logs

Inteligência na ponta dos seus dedos

Acesse nosso portal web, compatível com navegadores padrão, 24 horas por dia para informações em tempo real sobre ataques e suas severidades. Garantimos acessos a nossa plataforma a número ilimitado de colaboradores.

O portal oferece informações detalhadas sobre a origem dos ataques:

- **Países de Origem:** Identifique de onde vêm as ameaças.
- **Intervalos (Ranges) de Endereços IP:** Detalhes precisos sobre as fontes dos ataques.
- **Características e Tipos dos Ataques:** Classificação clara dos eventos (SYN flood, UDP flood, HTTP flood, etc.).
- **Data e Horário:** Registro completo de início e término dos ataques.
- **Volume de Tráfego:** Discriminação de tráfego bloqueado e não bloqueado por protocolo.
- **Alvos Afetados:** Identifique os recursos mais atacados (servidores, serviços, aplicativos).
- **Ofensores (Origem):** Conheça os IPs de origem dos ataques.
- **Classificação por Geolocalização:** Ofensores classificados por país, cidade ou região.
- **Percentual do Tráfego de Origem:** Detalhamento por continente ou região.
- **Taxa Média e Pico de Tráfego:** Medidas em Gbps e/ou Mpps.
- **Metodologia de Mitigação Empregada:** Entenda como cada ataque foi bloqueado (blackhole, rate limiting, challenge-response).
- **Alertas de Eventos Críticos:** Notificações detalhadas sobre a gravidade dos ataques.
- **Logs Detalhados para Auditoria:** Para sua total conformidade e análise.

Além disso, o portal permite a análise de pacotes tratados com visualização estilo “Wireshark” e download em formato PCAP, oferecendo uma visão aprofundada para sua equipe técnica.

A solução implementa e garante acesso de consulta (via portal ou SNMP v3) a Solução Anti-DDoS, proporcionando integração e controle completos.

4.3. Compromissos de Desempenho e Tempos de Resposta

Proteção com agilidade mensurável

Mais do que tecnologia, oferecemos compromissos claros e mensuráveis. Nossa solução opera com tempos de resposta definidos para cada cenário de acionamento, garantindo que a mitigação aconteça na velocidade que o seu negócio exige.

≤ 30 s	**Mitigação automática inline** Após a identificação de anormalidade no tráfego pelos nossos mecanismos de detecção, a mitigação de ataques DoS e/ou DDoS é iniciada em, no máximo, 30 (trinta) segundos, atuando em tempo real (inline).
≤ 5 min	**Mitigação sob solicitação** Quando o acionamento partir da equipe autorizada do cliente, a mitigação é iniciada em, no máximo, 5 (cinco) minutos após a solicitação, com o suporte integral do nosso SOC 24/7.
100 / 250 ms	**Latência controlada mesmo durante ataques** Nos períodos de ataque, a latência do circuito é de, no máximo, 100 ms (cem milissegundos) quando a mitigação se originar dos nossos centros de limpeza nacionais, e de, no máximo, 250 ms (duzentos e cinquenta milissegundos) quando se originar de centro(s) internacional(is). Sua operação permanece rápida, mesmo sob ataque.

HUGE NETWORKS · AS264409

Para mais informações, entre em contato com o seu Gerente de Contas.