



## 1. DESCRIÇÃO FUNCIONAL

A Mega é uma empresa líder no mercado de Tecnologias e de Telecomunicações, que oferece o melhor desses dois mundos, como uma única plataforma de soluções integradas para os seus clientes há mais de 25 anos.

O produto **Anti-DDoS** da **MEGA** opera sob o conceito de plataforma híbrida (Always On e Cloud), protegendo toda a rede da Mega e de seus clientes contra ataques **DoS** e **DDoS**.

A tecnologia adotada pela Mega para sua solução Anti-DDoS, fornece detecção baseada em comportamento que utiliza aprendizado de máquina para identificar automaticamente o tráfego de usuários legítimos e fornecer cobertura completa de proteção contra ataques DDoS tanto na camada de rede (L3/4) quanto na camada de aplicação (L7).

Os mecanismos patenteados de criação automática de assinaturas da Radware fornecem proteção automática em tempo real contra os ataques DDoS *zero-day* mais avançados, como ataques DDoS de rajada, ataques de IP dinâmico, ataques de botnet IoT, ataques DNS, Carpet Bombing e outros.

A tecnologia utilizada pela MEGA para o Anti-DDoS permite a integração híbrida perfeita entre o appliances DDoS on-premise e o serviço de nuvem, o que permite visibilidade, desvio automático e atualizações de políticas em todos os níveis.

O Serviço de Proteção DDoS em Nuvem da Mega oferece uma das maiores redes dedicadas de limpeza de DDoS da indústria, com alta capacidade e cobertura global.

Finalmente, a Mega oferece aos clientes visibilidade e gerenciamento completos com uma única interface, um único fornecedor, um único ponto de contato e uma interface de gerenciamento unificada.

### Por que a solução da Mega no modelo de plataforma híbrida?

Enquanto uma solução baseada em premissa depende estritamente de um appliance de hardware local e as soluções on-demand e always-on são puramente baseadas em nuvem, um modelo híbrido combina um appliance de hardware local com capacidade de 100Gbps *Always On* e expansível para *Cloud* em caso de um ataque volumétrico superior a 100Gbps e até 3Tbps.

Durante o curso normal dos negócios, o tráfego flui diretamente para o data center. O appliance local inspeciona o tráfego em busca de ataques e bloqueia a maioria deles. Se for detectado um ataque em larga escala, que pode sobrecarregar o dispositivo (ou até mesmo saturar completamente a conexão), o tráfego é desviado para um centro de limpeza na nuvem (Scrubbing Center). O centro de limpeza bloqueará o tráfego de ataque e enviará apenas o



tráfego limpo para o cliente. Uma vez que o ataque termina, o tráfego é redirecionado de volta para o dispositivo.

A proteção híbrida contra DDoS permite que as organizações aproveitem o melhor dos dois mundos: a baixa latência e o alto controle das soluções locais, junto com a capacidade escalável das soluções em nuvem.

Veja a tabela abaixo para uma comparação dos diferentes modelos de implementação:

	On-Premise	On-Demand	Always-On	Hybrid
Detection	Volumetric + nonvolumetric	Volumetric only	Volumetric + nonvolumetric	Volumetric + nonvolumetric
Latency	None in peacetime	None in peacetime	Minor added latency	None in peacetime
Protection	Immediate	Few min. until diversion	Immediate	Immediate
Capacity	Limited	High	High	High
Best For	Service providers Regulated industries	Service providers with many protected assets  Cost-sensitive enterprises not frequently attacked	Applications on public cloud  Organizations constantly attacked	Data center protection  Apps sensitive to latency  Mission-critical applications

## 2. VANTAGENS ANTI-DDOS HÍBRIDO

Existem muitas vantagens ao adotar uma solução híbrida para uma plataforma de proteção contra ataques DDoS, vejamos algumas a seguir:

### 2.1. Melhor qualidade da Proteção

A proteção híbrida é a prática recomendada pela maioria dos analistas de segurança, pois combina baixa latência e alta capacidade para a proteção de serviços críticos.

### 2.2. Detecção Imediata

Como o tráfego flui pelo appliance local o tempo todo, os ataques podem ser detectados imediatamente pelo dispositivo. Esta é uma vantagem sobre os serviços em nuvem sob demanda, que geralmente têm uma lacuna de detecção e proteção até que o desvio seja iniciado.

### 2.3. Capacidade Flexível



A disponibilidade de capacidade de mitigação flexível em caso de ataques volumétricos em grande escala é uma vantagem. Tais ataques podem sobrecarregar appliances de hardware autônomos e até saturar a conexão de internet que leva ao data center. Ter capacidade de backup na nuvem permite que os clientes lidem com qualquer ataque, independentemente do tamanho.

#### **2.4. Baixa Latência**

Soluções híbridas permitem baixa latência, já que a proteção no dia a dia é tratada por appliances locais diretamente no data center. Somente no momento de ataque o tráfego será desviado para a nuvem. Isso é uma vantagem em comparação com soluções em nuvem sempre ativas, que geralmente adicionam alguma latência às comunicações, mesmo durante períodos de baixo tráfego.

#### **2.5. Regulação**

Empresas em indústrias regulamentadas, como finanças, saúde e até mesmo Governo, frequentemente têm restrições e limitações em sua capacidade de migrar serviços para a nuvem. Portanto, uma solução híbrida pode ser útil ao fornecer proteção local na maior parte do tempo, enquanto ainda permite capacidade de backup em caso de ataques em grande escala.

#### **2.6. Controle**

Ter um dispositivo on-premise garante maior controle e configurabilidade, especialmente para organizações com topologias de rede únicas ou necessidades específicas.

---

### **3. ATRIBUTOS E FUNCIONALIDADES**

---

#### **3.1. Capacidade de Tráfego Legítimo**

O sistema de proteção Anti-DDoS da MEGA é projetado para lidar com um alto volume de tráfego legítimo garantindo que os usuários autorizados possam acessar os serviços sem interrupções, mesmo durante um ataque.

#### **3.2. Capacidade de Tráfego Mitigado**



A solução Anti-DDoS da MEGA pode mitigar ataques de até 3 Tbps, utilizando uma combinação de infraestrutura on-premises e em nuvem para garantir a proteção contra ataques volumétricos de grande escala.

### **3.3. Tempo de Notificação**

O sistema é capaz de detectar anomalias e enviar notificações em aproximadamente 15 minutos, garantindo uma resposta rápida a qualquer ameaça identificada.

### **3.4. Quantidade de Blocos IP Classe C Suportados**

A solução suporta a proteção de múltiplos blocos de endereços IP Classe C, permitindo que grandes redes sejam protegidas contra ataques DDoS.

### **3.5. Horário de Atenção**

O serviço de proteção Anti-DDoS da MEGA opera 24 horas por dia, 7 dias por semana, 365 dias por ano, garantindo monitoramento e mitigação contínuos.

### **3.6. Tempo para Início da Mitigação**

A mitigação de ataques é iniciada automaticamente em menos de 5 segundos após a detecção, assegurando a proteção imediata contra ameaças.

### **3.7. Serviço de SOC**

O Centro de Operações de Segurança (SOC) da MEGA monitora continuamente o tráfego e os alertas de segurança, utilizando ferramentas avançadas para identificar e responder rapidamente a ataques.

### **3.8. Serviço de Instalação**

A MEGA oferece serviços de instalação especializados para configurar a solução Anti-DDoS de acordo com as necessidades específicas de cada cliente, garantindo uma implementação eficiente e eficaz.

### **3.9. Relatórios de Ameaças Detectadas e Mitigadas**

Relatórios detalhados sobre as ameaças detectadas e mitigadas são gerados regularmente, fornecendo insights valiosos sobre a segurança da rede e ajudando na tomada de decisões informadas.



### 3.10. Inspeção Always On

A solução Anti-DDoS da MEGA oferece a opção "Always On", que proporciona proteção contínua on-premises para ataques DDoS com volume de até 100Gbps, garantindo que a rede esteja sempre protegida, independentemente do tipo de ataque.

### 3.11. Inspeção e Mitigação Cloud

A solução oferece capacidade de inspeção e mitigação na nuvem, onde o tráfego pode ser desviado para centros de limpeza em nuvem da MEGA em caso de ataques volumétricos que excedam a capacidade dos dispositivos on-premises, com capacidade de mitigar ataques de até 3 Tbps.

### 3.12. Tipos de Ataques Mitigados

A solução é capaz de mitigar uma ampla gama de ataques DDoS, incluindo:

- Ataques de rede (camada L3/4)

<b>Tipos de Ataques e Algoritmos Suportados L3/L4</b>
Black Filter Lists
White Filter Lists
GEOIP Filter Lists
Drop based on country
Access Control Lists Filtering
Anti-spoofing
IP Behavior Analysis
Trusted Source IP Control
Malformed IP Header
Bad IP Checksum
Short Packet
IP Location Policing
Zombie Detection
NTP Flood/Reflection/Amplification
SNMP Flood/Reflection/Amplification
ICMP Flood
Generic UDP floods
TCP Source Port 0
TCP Destination Port 0
TCP Regular Expression Filtering
UDP Regular Expression Filtering
SYesN Check
ACK Check
TCP SYesN Source IP Rate Limit



TCP SYesN Source Bandwidth Limit
TCP SYesN Destination Bandwidth Limit
TCP SYesN Time Sequence Check
DNS Flood/Reflection/Amplification
Port Check
TCP Fragment Control
ICMP Fragment Control
UDP Source Port 0
TCP Destination Port 0
UDP Payload Check
UDP Fragment Control
UDP Packet Length Check
UDP Traffic Control
Incomplete Fragment
Duplicate Fragment
Fragment Too Long
Short TCP Packet
Short UDP Packet
Short ICMP Packet
Bad TCP / UDP Checksum
Invalid TCP Flags
Invalid ACK Number
Bad TCP check
SYesN Floods
TCP SYesN Authentication
Out-of-sequence Authentication
TCP Connection Limiting
TCP Connection Idle Timeout
UPnP
RDP
Source Based Mitigation
UBNT Exploit
GRE Flood
Mitigation based on PDU length
Invalid Packets
Layer 4 RFC Violation
<i>ADDP Reflection</i>
<i>Andrew File System (AFS) Reflection</i>
<i>APDoS</i>
<i>ARD Reflection</i>
<i>Bittorrent DHT Reflection</i>
<i>Citrix Legacy IMA Service Reflection</i>
<i>cLDAP</i>
<i>CoAP Amplification</i>
<i>CVE-2018-5400 Vuln Ref</i>



CWE-406
DNS Query Flood
DTLS Reflection
DVR DHCPDiscover
Fork Bomb
Fraggle Attack
Jenkins (Hudson Agent) Reflection
Lantronix IoT
MemcacheD Reflection
MS SQL Reflection
Multi Vector Attacks
NetBIS Service Reflection
Netcore/Netis Routers Vuln
Nuke Attack
OpenVPN dynamic servers reputation
OpenVPN dynamic users reputation
OpenVPN Reflection
p2p Attack
Plex Media Server (patched**)
QOTD Reflection
QUIC Amplification
R.U.D.Yes.
Restund & CoTURN Reflection
Sentinel (RMS License Manager) Amplification
SIP Amplification
SNMPv2 Reflection
Spoofed Session
SSDP Reflection
SSL Negotiation Attack
Synonymous IP
TCP PSH Flood
Teardrop
TP240 Reflection
vxWorks Reflection
WS-DD
XDMCP Reflection

- Ataques de aplicação (camada L7)

<b>Tipo de Algoritmos e Ataques Suportados L7</b>
Reflection Amplification Rules
Connection Exhaustion
URL-ACK Filter Lists
DNS Keyword Checking
DNS Rate-Limiting
DNS TCP-BIT Check





DNS CNAME Check
DNS Retransmission
HTTP Keyword Checking
HTTP Authentication
HTTP Dynamic Script
HTTP FCS Check
HTTP Pattern Matching Check
HTTP Slow Attack Check
Empty Connection Check
HTTPS SSL Connection Control
HTTPS Authentication
SIP Authentication
Blacklist Fingerprints

### 3.13. Proteção de Blocos de Rede e ASN de Terceiros

Além de proteger os próprios blocos de IP associados ao seu ASN, a solução da MEGA oferece a capacidade de estender a proteção para blocos de rede e ASN de terceiros. Isso permite que organizações protejam não apenas sua própria infraestrutura, mas também a de parceiros ou clientes que compartilham recursos de rede.

### 3.14. Suporte IPv4 e IPv6

A solução da MEGA oferece suporte completo para tráfego IPv4 e IPv6, garantindo que organizações com infraestruturas mistas possam se beneficiar da proteção contra ataques DDoS em ambas as versões de protocolo.

### 3.15. Mitigação Inteligente

A solução Anti-DDoS da MEGA inclui recursos de Mitigação Inteligente, onde os sistemas são capazes de distinguir tráfego malicioso de tráfego legítimo com maior precisão. Isso é realizado através da análise detalhada do comportamento do tráfego e da aplicação de políticas de mitigação específicas para cada tipo de ataque, garantindo que apenas o tráfego nocivo seja bloqueado, enquanto o tráfego legítimo continua fluindo sem interrupções.

---

## 4. SOC – SECURITY OPERATION CENTER

---

### 4.1. Monitoramento Contínuo

O Centro de Operações de Segurança da MEGA monitora continuamente, 24 horas por dia, 7 dias por semana, durante todo o ano todos os aspectos da rede e dos sistemas de seus clientes. Utilizando ferramentas avançadas de monitoramento de flows e ameaças cibernéticas, o SOC identifica rapidamente atividades suspeitas ou ataques em potencial.



#### **4.2. Resposta a Incidentes**

Em caso de detecção de ameaças, o SOC da MEGA possui procedimentos definidos para responder rapidamente. Isso inclui a coordenação com equipes internas e, se necessário, com clientes para mitigar o impacto de incidentes de segurança.

#### **4.3. Análise Forense e Relatórios**

Além de responder a incidentes em tempo real, o SOC realiza análises forenses detalhadas para entender a origem e o impacto de ataques passados. Relatórios completos são gerados para ajudar os clientes a entender as ameaças enfrentadas e tomar medidas preventivas.

#### **4.4. Geração automática de alertas e caracterização de ataques**

O processo de monitoramento permite a geração rápida de alertas no sistema. Esses alertas são baseados nas informações de padrão de tráfego de linha base coletados pela plataforma anti-ddos da Mega durante o período de análise. Utilizando esses dados, é possível determinar se a anomalia corresponde a um uso válido do serviço de Internet, se o tipo de tráfego recebido está alinhado com os serviços publicados pelo CONTRATANTE, entre outras características. Isso permite que a MEGA priorize adequadamente os alertas gerados, classificando-os como de baixa, média ou crítica prioridade.

#### **4.5. Filtragem inteligente dos ataques DDoS Volumétricos**

Quando os alertas atingem o nível crítico, o sistema realiza uma filtragem inteligente do tráfego, separando o tráfego associado ao ataque DDoS do restante do tráfego consumido pelo CONTRATANTE. Esse tráfego identificado como malicioso é então encaminhado para análise detalhada no sistema, que examina pacote por pacote utilizando uma base de dados especializada contendo assinaturas de ataques conhecidos globalmente.

Durante essa análise, o sistema compara cada pacote com os perfis de ataques previamente registrados. Os pacotes que correspondem a esses perfis são descartados imediatamente, protegendo assim os pacotes legítimos e suavizando o impacto do ataque.

#### **4.6. Geração de Relatórios**

O sistema permite extrair informações detalhadas dos alertas gerados, do tráfego analisado e dos ataques mitigados. A MEGA tem à sua disposição todos os dados necessários para criar relatórios completos sobre sua gestão frente aos ataques volumétricos de negação de serviço.



---

## 5. ESCOPO DO PRODUTO

---

O serviço de proteção contra ataques DDoS da Mega está disponível no Brasil e com atendimento local.

A seguir é apresentado o escopo do serviço Anti-DDoS oferecido pela Mega :

- O serviço prove proteção completa contra ataques DDoS, o que significa que o tráfego malicioso será identificado e bloqueado antes de afetar o desempenho do site ou aplicação;
- No processo de implantação do projeto será incluído a parametrização inicial do serviço, com a qual se agiliza o processo de alerta e mitigação dos ataques;
- Sem limite de mitigações por mês. O número de eventos de mitigação será ilimitado durante o mês dentro do tamanho máximo da linha de base de proteção (commitment);
- Sem limite de adição de subredes classe C;
- Sem limite de tempo de duração de ataques;
- Atendimento do SOC é 24x7 e a ferramenta dispara automaticamente os gatilhos de mitigação na plataforma, imediatamente após identificar um evento considerado malicioso;
- A linha de base de proteção é definida equivalente ao tráfego legítimo (limpo) e a capacidade de Internet contratada com a MEGA, excluindo a capacidade excedente a qual será considerada como burstable.

---

## 6. IMPLANTAÇÃO DO SERVIÇO

---

O produto Anti-DDoS da Mega é um ecossistema que requer a implementação de diversos passos essenciais. É fundamental que o cliente participe ativamente de todo o processo de implantação da solução. O sucesso da implementação depende da cooperação do cliente com os processos estabelecidos abaixo. O prazo de implementação será definido durante o Kick-off do projeto junto ao cliente.

As seguintes atividades devem ser executadas:

### 6.1. Atividades a serem Executadas:

- Instalação do link de IP Trânsito ou Internet Dedicado;
- Preenchimento adequado do formulário de ativação da plataforma;
- Início do Learning Mode para aprendizado do padrão de tráfego do cliente;
- Estabelecimento das sessões BGP (quando aplicável)
- Acompanhamento pós-ativação.

### 6.2. Premissas e Condições para ativação:

- A proteção Anti-DDoS tem um período de estabilidade de 3 semanas, durante o qual a plataforma utilizada para a filtragem do tráfego reconhece os padrões normais de tráfego do CONTRATANTE a fim de ajustar o processo de caracterização do tráfego malicioso.



Durante essas 3 semanas, o serviço pode levar mais tempo que o estabelecido para gerar os alertas ou pode, até mesmo, não gerar alertas para alguns ataques específicos;

- O CONTRATANTE deve fornecer de forma completa e exata todas as informações exigidas pela MEGA na etapa da pré-venda, a fim de obter uma proteção ágil e eficiente; parte imprescindível desta informação são os blocos de subrede classe C, bem como o ASN associado a esta rede.
- Durante o processo de mitigação de um ataque DDoS, o fluxo de rede direcionado a um host sob ataque pode experimentar maior latência devido ao processo de verificação que ocorre antes de ser entregue ao destino.
- A proteção Anti-DDoS é aplicada somente para os blocos de endereços IP que estejam cadastrados no sistema Anti-DDoS da MEGA e declarados na contratação do serviço. Caso o CONTRATANTE solicite a modificação dos endereços protegidos, deve-se levar em consideração o tempo adicional que envolve este trabalho e adicioná-los ao processo normal de mitigação de ataques através de formulário específico.
- A MEGA não compartilha com seus clientes os alertas gerados pelo sistema, mas sim os relatórios relacionados com os ataques mitigados e os relatórios periódicos nos quais se evidencia a gestão feita pela MEGA dentro deste escopo.
- A proteção Anti-DDoS é fornecida junto com o serviço IP Trânsito ou Internet Dedicado da MEGA, portanto, não é possível oferecer esta proteção quando a MEGA não é o fornecedor de trânsito IP do CONTRATANTE.
- Embora a MEGA garanta a gestão do serviço através de pessoal qualificado e certificado e com tecnologia de ponta, ao enfrentar ataques de negação de serviço, talvez não seja possível garantir a completa eficácia das técnicas de mitigação e dos procedimentos de segurança estabelecidos devido à alta complexidade dos ataques e à rápida evolução das técnicas utilizadas pelos cybers criminosos.

---

## 7. ARQUITETURA

---

A proteção Anti-DDoS é baseada na administração de um sistema formado por uma plataforma que faz monitoramento constante do tráfego que passa através da rede da MEGA e por uma plataforma complementar que analisa em detalhe os pacotes para descartar os que tenham conteúdo malicioso. A MEGA conta com estes elementos que estão instaladas em São Paulo, no Brasil.

A plataforma é capaz de identificar e mitigar ataques com origem de conexões provenientes de peering diretos com CDNs (Content Delivery Networks) e IXP (Internet Exchange Point), além dos provedores de transito Tier 1.

O Anti-DDoS Cloud da MEGA possui centros de mitigação (Scrubbing Centers) em todos os continentes, garantindo que os ataques sejam mitigados o mais próximo possível da origem do ataque. Além de centros de mitigação distribuído pelo mundo, nosso centro de mitigação de ataques DDoS em São Paulo, possibilita aos nossos clientes brasileiros a menor taxa de latência no retorno do tráfego limpo.

