

## Manual Funcional Anti-DDoS – Net Express Brasil.

### 1. OBJETIVO E VISÃO GERAL

Este manual descreve, de forma objetiva, o funcionamento do serviço Anti-DDoS fornecido pela NET EXPRESS BRASIL, bem como seus principais recursos, capacidades e premissas operacionais.

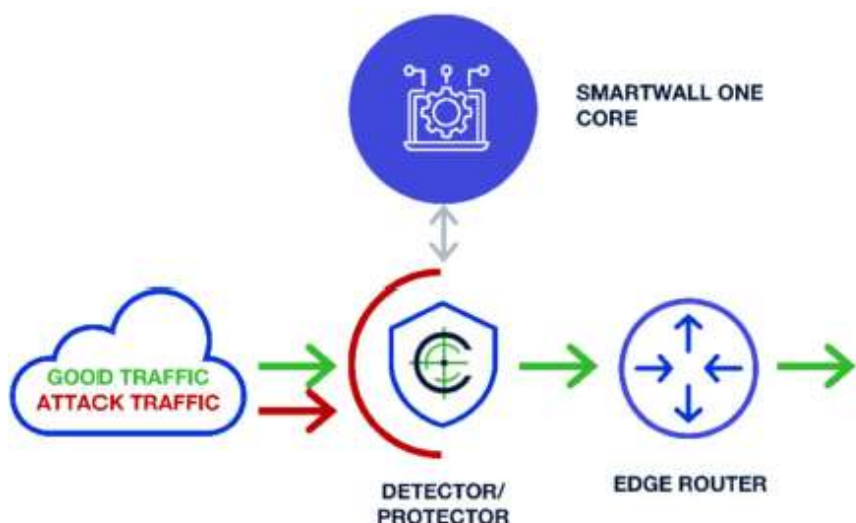
A solução foi desenhada para proteger serviços críticos de conectividade e aplicações expostas à Internet, assegurando continuidade operacional mesmo diante de ataques de negação de serviço (DoS/DDoS) em camadas de rede (L3/L4) e aplicação (L7).

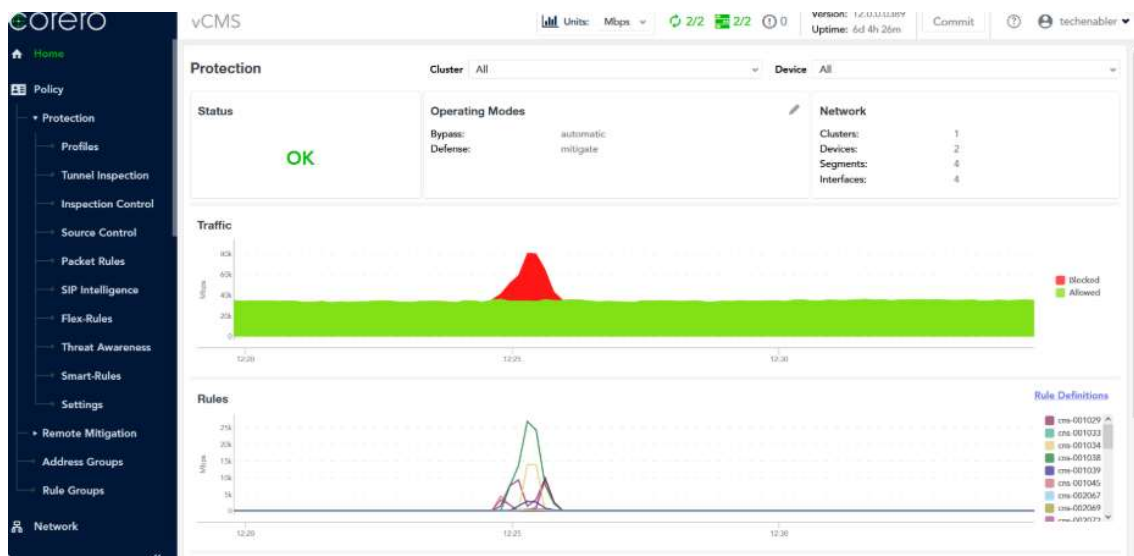
### 2. ARQUITETURA DO SERVIÇO (MODELO HÍBRIDO)

A NET EXPRESS BRASIL opera o Anti-DDoS em modelo híbrido, combinando mitigação local (Always-On) com capacidade adicional de mitigação em Scrubbing Center (Cloud) para cenários de ataques volumétricos acima da capacidade do ambiente local.

No funcionamento normal, o tráfego segue seu caminho natural dentro do backbone da NET EXPRESS BRASIL, com inspeção e mitigação contínuas realizadas pelo appliance CORERO instalado em ambiente de datacenter. Em eventos de grande escala, o tráfego pode ser direcionado para limpeza em Scrubbing Center, retornando ao destino apenas após remoção do tráfego malicioso.

Esse modelo permite manter baixa latência e alto controle no dia a dia, ao mesmo tempo em que garante escalabilidade para ataques de alta intensidade.





### 3. PRINCIPAIS BENEFÍCIOS

#### 3.1 Detecção rápida e mitigação automática

Como a inspeção ocorre em modo Always-On, a identificação de anomalias é imediata e a mitigação pode ser acionada automaticamente, reduzindo o tempo de exposição.

#### 3.2 Continuidade do serviço

O serviço é projetado para preservar o tráfego legítimo, mantendo o acesso dos usuários autorizados mesmo durante ataques.

#### 3.3 Baixa latência

A mitigação local evita aumento desnecessário de latência em períodos sem ataque, diferentemente de modelos puramente “cloud always-on”.

#### 3.4 Capacidade escalável

Em ataques que excedam a capacidade local, a camada de Scrubbing Center complementa a proteção, permitindo absorção de volumes superiores.

### 3.5 Adequação para ambientes críticos e regulados

A arquitetura híbrida atende ambientes com exigência de controle e requisitos de segurança elevados, incluindo órgãos públicos e empresas com serviços essenciais.

## 4. ATRIBUTOS E FUNCIONALIDADES

### 4.1 Capacidade de tráfego legítimo

A plataforma é dimensionada para suportar altos volumes de tráfego legítimo, evitando bloqueios indevidos e garantindo estabilidade do serviço.

### 4.2 Capacidade de mitigação

A solução combina mitigação local com capacidade adicional em Scrubbing Center, permitindo proteção contra ataques volumétricos e multivetoriais.

### 4.3 Operação 24x7

A operação do serviço é contínua (24 horas por dia, 7 dias por semana, 365 dias por ano), com monitoramento e resposta a incidentes.

### 4.4 Relatórios e evidências

A NET EXPRESS BRASIL pode emitir relatórios periódicos e sob demanda contendo informações de ataques detectados, mitigados e métricas de impacto e resposta.

## 5. TIPOS DE ATAQUES COBERTOS

A solução Anti-DDoS da NET EXPRESS BRASIL (CORERO) possui mecanismos de proteção contra múltiplas técnicas de ataque, incluindo, mas não se limitando a:

- Floods e amplificações (DNS/NTP/SSDP, entre outros)
- Ataques TCP (SYN/ACK/PSH, exaustão de conexões)
- Ataques UDP genéricos e direcionados
- Ataques multivetoriais e variações de botnets
- Ataques em camada de aplicação (L7), conforme políticas configuradas

## 6. PROCESSO DE IMPLANTAÇÃO (VISÃO OPERACIONAL)

A implantação do serviço Anti-DDoS envolve as seguintes etapas:

- 1) Levantamento técnico e validação dos endereços/prefixos a serem protegidos;
- 2) Parametrização inicial e ativação do ambiente;
- 3) Período de aprendizado (learning mode) para estabelecimento de baseline;
- 4) Ajustes finos de políticas e validação de mitigação;
- 5) Entrada em operação assistida e acompanhamento pós-ativação.

O prazo e o detalhamento final são definidos em reunião de kick-off com o cliente.

## 7. PREMISSAS E CONDIÇÕES IMPORTANTES

- A proteção Anti-DDoS é aplicada apenas aos endereços IP/prefixos previamente cadastrados no serviço.
- Durante mitigação, pode ocorrer variação de latência devido ao processamento de inspeção e filtragem.
- Em cenários extremos, a efetividade depende do volume, da complexidade do ataque e da disponibilidade de capacidade de transporte.
- O serviço Anti-DDoS é ofertado de forma integrada à conectividade IP fornecida pela NET EXPRESS BRASIL, garantindo operação e acionamento dentro do mesmo fornecedor.

## 8. SUPORTE E ATENDIMENTO

O suporte técnico é realizado diretamente pelo SOC da NET EXPRESS BRASIL, por meio de:

- **Telefone:** 0800 001 6644
- **E-mail:** [soc@netexpressbrasil.com](mailto:soc@netexpressbrasil.com) e [noc@netexpressbrasil.com](mailto:noc@netexpressbrasil.com)

Atendimento **24x7x365**.

Também será disponibilizado à contratante o **Portal do SOC**, permitindo o acompanhamento dos tipos de ataques e das mitigações realizadas.

