

ESTRATÉGIA DE MITIGAÇÃO DE ATAQUES DDoS

SENADO FEDERAL

PREGÃO ELETRÔNICO Nº 90130/2025

PROCESSO ADMINISTRATIVO Nº 00200.011885/2025-82

1. IDENTIFICAÇÃO DA PROPONENTE

A **NET EXPRESS BRASIL**, com sede no **Setor de Habitações Individuais Sul – QI 5, Qd. B, Bloco B, Sala 201, Lago Sul, Brasília/DF, CEP 71615-720**, inscrita no CNPJ nº **24.857.944/0001-48**, telefone **(61) 4063-7071**, por intermédio de seu representante legal **Sr. Ricardo Pires Rodrigues**, portador da Carteira de Identidade nº **2.529.342** e CPF nº **002.952.871-28**, apresenta a presente **ESTRATÉGIA DE MITIGAÇÃO DE ATAQUES DDoS**, para atendimento ao **PREGÃO ELETRÔNICO Nº 90130/2025**, conforme as especificações a seguir.

2. DECLARAÇÃO DE CAPACIDADE OPERACIONAL

Declaramos que a **NET EXPRESS BRASIL** possui **03 (três) Centros Operacionais de Segurança – SOC (Security Operations Center) no Brasil**, compostos por equipes especializadas em:

- Monitoramento contínuo
- Detecção de ameaças
- Mitigação de ataques de negação de serviço distribuído (DDoS)

O atendimento é realizado:

- **24 (vinte e quatro) horas por dia**
- **07 (sete) dias por semana**
- **365 (trezentos e sessenta e cinco) dias por ano**
- Em idioma português brasileiro
- Por meio de **telefone 0800, correio eletrônico e portal do cliente**

Durante todo o período de vigência contratual.

3. VISÃO GERAL DA ESTRATÉGIA DE MITIGAÇÃO

A estratégia adotada parte da **análise do perfil do contratante**, permitindo a definição antecipada das melhores práticas de segurança, garantindo **monitoramento, detecção e mitigação eficazes**.

Todos os incidentes são tratados diretamente pelos **Centros Operacionais de Segurança da NET EXPRESS BRASIL**, sendo de responsabilidade exclusiva de sua equipe a mitigação de quaisquer ataques DDoS identificados.

Atualmente, os centros de mitigação utilizam a solução **CORERO NTD 3400**, reconhecida internacionalmente por sua eficiência, rapidez e inteligência no combate a ataques de grande escala.

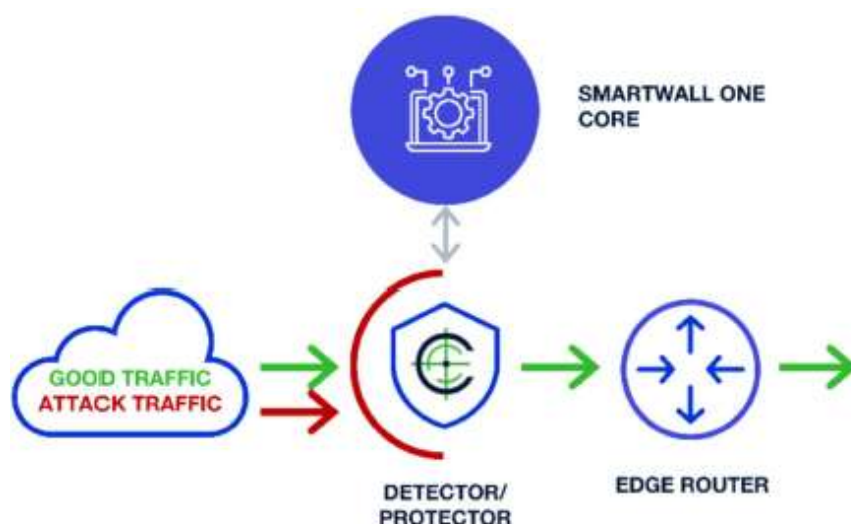
A solução atua de forma **proativa**, iniciando a mitigação **em até 15 (quinze) minutos após a detecção do ataque**, analisando pacote a pacote, removendo tráfego malicioso e permitindo apenas a passagem do tráfego legítimo até o destino final.

4. ARQUITETURA DE TRÁFEGO E MITIGAÇÃO

O fluxo de tráfego na rede ocorre da seguinte forma:

- **Inline deployments**

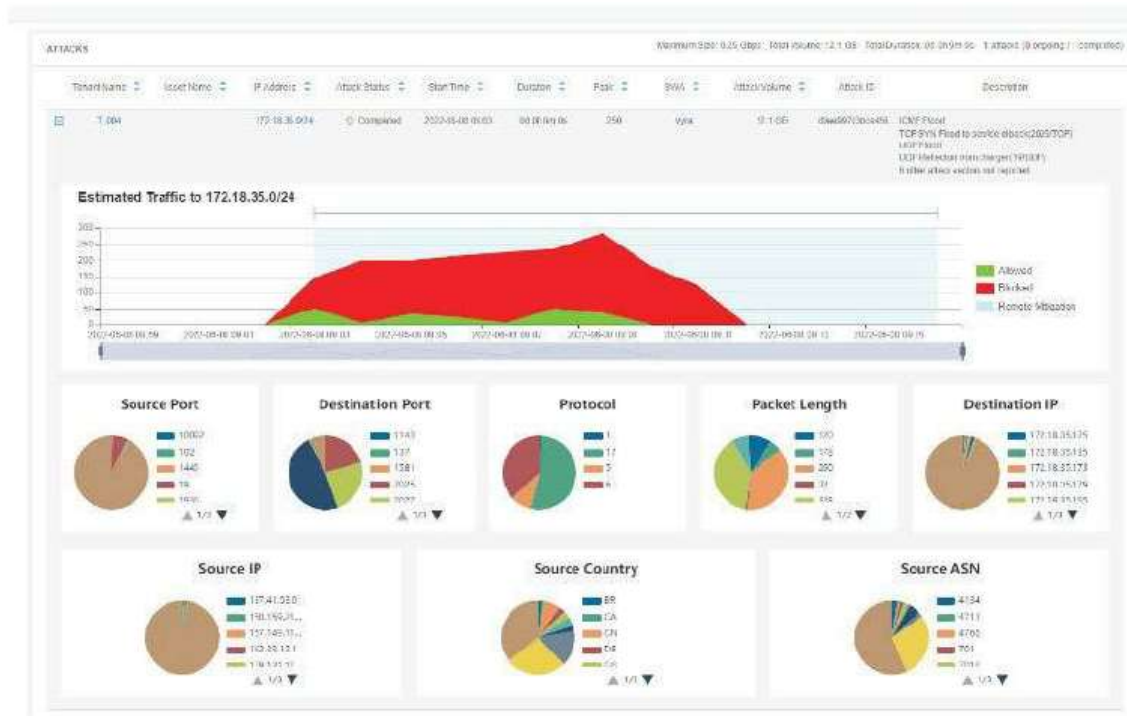
Caminho nativo do tráfego entre origem e destino, definido pelos protocolos de roteamento.



5. ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO – CORERO NTD 3400

5.1 Proteção Inteligente contra DDoS

- Detecção e bloqueio de ataques DDoS volumétricos, inclusive **zero-day**
- Regras comportamentais para identificação de padrões anômalos em tempo real
- Bloqueio preciso de vetores conhecidos sem impacto ao tráfego legítimo
- Inteligência preditiva baseada em feeds globais de ameaças
- Detecção e bloqueio de ataques originados de botnets
- Bloqueio automático de fragmentações maliciosas
- Políticas de controle de taxa por porta TCP/UDP
- Integração com mitigação em nuvem e sinalização **BGP RTBH / FlowSpec**



5.2 Proteção contra Exaustão de Recursos

- Bloqueio de pacotes malformados ou truncados (UDP bombs)
- Mitigação de ataques por fragmentação e segmentação IP
- Validação de sessões TCP e identificação de pacotes inválidos
- Detecção de flags ilegais e checksums incorretos
- Proteção contra uso indevido de portas TCP/UDP
- Defesa contra ataques DNS do tipo **NXDOMAIN Water Torture**

5.3 Defesa contra Ataques Volumétricos

- TCP Flood
- UDP Flood
- Fragmentação UDP
- SYN Flood
- ICMP Flood
- Carpet Bombing

5.4 Mitigação de Ataques por Amplificação e Reflexão

- Amplificação NTP (monlist)
 - Amplificação DNS
 - CLDAP (LDAP sem conexão)
 - SSDP / UPnP
 - Respostas SNMP
 - CHARGEN
-

6. BENEFÍCIOS AO SENADO FEDERAL

- Alta disponibilidade dos serviços, mesmo sob ataque
 - Redução de indisponibilidade e impactos operacionais
 - Proteção automática, sem necessidade de intervenção manual
 - Solução escalável para ambientes de alta capacidade
 - Segurança sem impacto na experiência dos usuários finais
-

7. 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

Atendimento **24x7x365**.

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



8. CAPACIDADE GLOBAL DE MITIGAÇÃO

- 15 centros globais de mitigação inteligentes
- Mais de **85 Tbps** de capacidade FlowSpec
- Interconexão com mais de **9.000 AS**
- Mais de **120 Tbps** de capacidade de rede
- Mitigação distribuída em mais de **500 localidades**
- Atualizações de contramedidas a cada **15 minutos** pelo **Black Lotus Labs**
- Mitigação iniciada em até **1 segundo** após o tráfego atingir os centros de limpeza

9. DATA CENTERS UTILIZADOS

9.1 ELEA DIGITAL – Brasília/DF

SIG Quadra 02, Lote 470 – CEP 70610-420

Confiabilidade:

Disponibilidade de **99,99%**

Infraestrutura:

- Piso elevado (1.200 kg/m²)
- Energia redundante (UPS N+1, geradores N+1)
- Refrigeração redundante
- SDACI com VESDA, gás e sistema pré-action

Segurança:

- 4 níveis de controle de acesso
 - Segurança humana 24h
 - Controle eletrônico por cartão de proximidade
-

9.2 EQUINIX SP4 – Barueri/SP

Av. Ceci, 1900 – Res. Tamboré – CEP 06460-120


Infraestrutura certificada conforme:

- ISO 9001
 - ISO 27001
 - SSAE 16 / ISAE 3402 SOC 1
 - PCI DSS
-

10. CONSIDERAÇÕES FINAIS

A NET EXPRESS BRASIL reafirma seu compromisso com a **segurança, disponibilidade e continuidade dos serviços**, colocando à disposição do SENADO FEDERAL uma solução robusta, comprovada e alinhada às melhores práticas internacionais de mitigação de ataques DDoS.

Brasília, 21 de janeiro de 2026.



Ricardo Pires Rodrigues
Sócio-Administrador
RG. 2.529.342 SSP/DF
CPF 002.952.871-28