



---

## **Caderno de Testes**

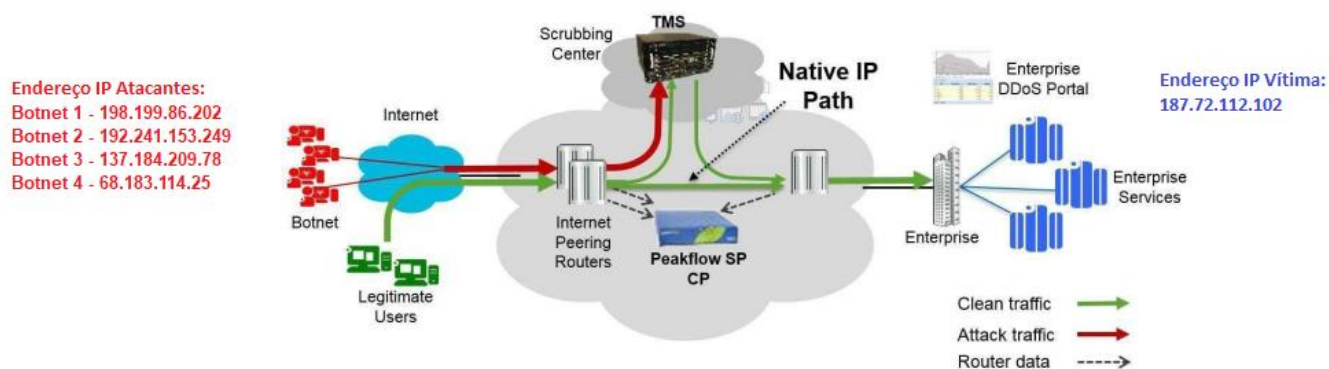
**Gerenciamento de Segurança –Anti DDoS**

---

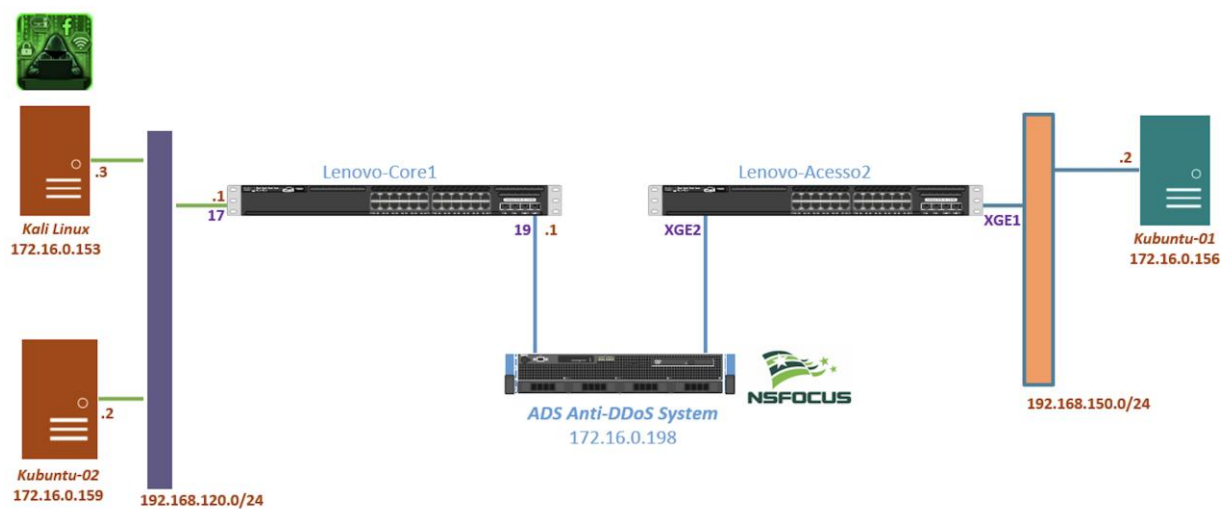
## Sumário

<b>Topologia (Volumétrico) .....</b>	<b>3</b>
<b>Topologia (Não-Volumétrico) .....</b>	<b>3</b>
<b>Caderno de Testes (Volumétrico) .....</b>	<b>4</b>
<b>Descrição da Ferramenta de Ataque .....</b>	<b>4</b>
<b>Mitigação de Ataques e Filtragem de Tráfego Ilegítimo sem Prejudicar Tráfego Legítimo .....</b>	<b>4</b>
<b>Mitigação Automatizada de Ataques DoS/DDoS na Nuvem com Redirecionamento de Tráfego .....</b>	<b>5</b>
<b>Suporte à Mitigação Automática de Ataques com Múltiplas Técnicas .....</b>	<b>5</b>
<b>Caderno de Testes (Não-Volumétrico) .....</b>	<b>7</b>
<b>Continuidade do Tráfego sem Interrupções por Falhas de Hardware .....</b>	<b>7</b>
<b>Mitigação de Ataques e Filtragem de Tráfego Ilegítimo sem Prejudicar Tráfego Legítimo .....</b>	<b>7</b>
<b>Mitigação Automática de Ataques com Limitação de Taxa de Tráfego .....</b>	<b>8</b>
<b>Deteção e Mitigação de Ataques DoS/DDoS em IPv4 e IPv6, Incluindo Camada de Aplicação .....</b>	<b>8</b>

## Topologia (Volumétrico)



## Topologia (Não-Volumétrico)



## Caderno de Testes (Volumétrico)

### Descrição da Ferramenta de Ataque

Foi criada uma ferramenta para automação dos ataques simulando uma visão real de inundação de pacotes gerando a volumetria necessária para demonstração e comprimento dos requisitos.

A partir da ferramenta foi possível gerar ataques serializados ou concorrentes com o comando hping3.

Para gerar o tráfego IPSEC foi criado um replay de um pacote válido IKE e então com o PCAP foi utilizado para o envio de requisições e gerar o tráfego flood neste protocolo.

Traffic Type	Commands
ICMP	hping3 -i u1 --icmp -d 1450 <i>dst.addr</i> --flood
TCP SYN	hping3 -i u1 -S -p 23 -d 1450 <i>dst.addr</i> --flood
TCP ACK	hping3 -i u1 -A -p 23 -d 1450 <i>dst.addr</i> --flood
UDP	hping3 -i u1 --udp -p 23 -d 1450 <i>dst.addr</i> --flood
IPSEC	./replay --fname /root/traffic.pcap --workers 100

### Mitigação de Ataques e Filtragem de Tráfego Ilegítimo sem Prejudicar Tráfego Legítimo

*Mitigação de ataques e limpeza do tráfego ilegítimo sem impedir/prejudicar o tráfego legítimo, sejam eles originados de um ou mais endereços IPs, mesmo que esses tenham sido originados através de, por exemplo, um proxy, NAT ou CGNAT.*

**Método Utilizado:** Durante a reprodução do ataque de negação de serviço TCP SYN, identificado no alerta ID 2523800, foi a conexão através de um acesso legítimo partindo de um dos Endereços IP's Atacantes.

Evidências disponíveis nos seguintes arquivos:

- [Figura 15 – Identificação do alerta 2523800 - Black Lists](#)
- [Figura 16 - alerta 2523800, detalhes mitigação e IP ofensores](#)
- [Figura 17 - alerta 2523800, detalhes mitigação por TMS e Deny-Allow Lists desabilitado](#)
- [Figura 18 - alerta 2523800, tráfego anômalo negado, requisições validas sem impacto](#)
- [Ataque do Alerta 2523800 + Requisição Válida Durante o Ataque](#)

## Mitigação Automatizada de Ataques DoS/DDoS na Nuvem com Redirecionamento de Tráfego

*O serviço é ser capaz de mitigar ataques de DoS/DDoS na nuvem de forma automatizada, configurando thresholds diferenciados para os níveis de proteção criados que, se atingidos, redirecionem o tráfego para o centro de limpeza da CONTRATADA, para posterior devolução do tráfego limpo à rede da CONTRATANTE.*

**Método Utilizado:** A solução está configurada de forma automática, assim que inicia um tráfego anômalo, após de alguns minutos, já é possível acompanhar os gráficos que demonstra:

- Tráfego em vermelho para o TMS (mitigador) em ação de forma automática sem ação humana.
- Tipos de ataques identificados, volume do tráfego anômalo em Gbps e pps mitigados entre outras.

Foram coletadas as evidências dos comandos realizados no Router de borda e dos eventos relacionados aos Alertas da plataforma de Anti-DDoS identificado no alerta ID 2524054, para evidenciar o desvio de rota dentro do Backbone ALGAR.

Evidências disponíveis nos seguintes arquivos:

- [Figura 21 - Tracerout - Antes do Desvio \(BGP\)](#)
- [Figura 22 - Tracerout - Depois do Desvio para o TMS \(BGP\)](#)
- [Figura 15 - Identificação do alerta 2523800](#)
- [Figura 16 - alerta 2523800, detalhes mitigação e IP ofensores](#)

## Suporte à Mitigação Automática de Ataques com Múltiplas Técnicas

*O serviço possui suporte à mitigação automática de ataques, utilizando múltiplas técnicas e inclui no mínimo: Black lists; ICMP flood; IPsec flood; TCP flood e UDP flood.*

**Método Utilizado:** Foi realizado um teste através de um ataque de negação de serviço a fim de demonstrar que a plataforma utiliza, como uma das contramedidas, a realização de mitigação utilizado Black Lists. Foi identificado uma tráfego anômalo com característica TCP SYN, identificado no alerta ID 2523419 com a intensão de verificar o ofensor na Black List.

**Método Utilizado:** Foi realizado um teste através de um ataque de negação de serviço a fim de demonstrar que a plataforma utiliza, como uma das contramedidas, a realização de mitigação utilizado o vetor ICMP flood. Foi identificado uma tráfego anômalo com característica ICMP flood, identificado no alerta ID 2523236.

**Método Utilizado:** Foi realizado um teste através de um ataque de negação de serviço a fim de demonstrar que a plataforma utiliza, como uma das contramedidas, a realização de mitigação utilizado o vetor IPsec flood. Foi identificado uma tráfego anômalo com característica IPsec flood, identificado no alerta ID 2523379.

**Método Utilizado:** Foi realizado um teste através de um ataque de negação de serviço a fim de demonstrar que a plataforma utiliza, como uma das contramedidas, a realização de mitigação utilizado o vetor TCP flood. Foi identificado uma tráfego anômalo com característica TCP SYN, identificado no alerta ID 2523262 e TCP ACK, identificado no alerta ID 2523283.

**Método Utilizado:** Foi realizado um teste através de um ataque de negação de serviço a fim de demonstrar que a plataforma utiliza, como uma das contramedidas, a realização de mitigação utilizando o vetor UDP flood. Foi identificado uma tráfego anômalo com característica UDP flood, identificado no alerta ID 2523350.

Evidências disponíveis nos seguintes arquivos:

- [Figura 12 – Identificação do alerta 2523419](#)
- [Figura 13 - alerta 2523419, detalhes mitigação e IP ofensores](#)
- [Figura 14 - alerta 2523419, detalhes mitigação e verificação drop Deny-Allow Lists](#)
- [Figura 1 – Identificação do alerta 2523236](#)
- [Figura 2 - alerta 2523236, detalhes mitigação e IP ofensores](#)
- [Ataque ICMP flood](#)
- [Figura 9 – Identificação do alerta 2523379](#)
- [Figura 10 - alerta 2523379, detalhes mitigação e IP ofensores](#)
- [Figura 11 - alerta 2523379, detalhes mitigação e verificação do pacote IPsec](#)
- [Ataque IPsec flood](#)
- [Figura 3 – Identificação do alerta 2523262](#)
- [Figura 4 - alerta 2523262, detalhes mitigação e IP ofensores](#)
- [Figura 5 – Identificação do alerta 2523283](#)
- [Figura 6 - alerta 2523283, detalhes mitigação e IP ofensores](#)
- [Ataque TCP ACK flood](#)
- [Ataque TCP SYN flood](#)
- [Figura 7 – Identificação do alerta 2523350](#)
- [Figura 8 - alerta 2523350, detalhes mitigação e IP ofensores](#)
- [Ataque UDP flood](#)

## Caderno de Testes (Não-Volumétrico)

### Continuidade do Tráfego sem Interrupções por Falhas de Hardware

*O tráfego da não sofre intermitências/interrupções por causa de quaisquer falhas de hardware de eventuais recursos tecnológicos instalados pela CONTRATADA nas dependências da CONTRATANTE.*

**Método Utilizado:** Foi realizada a reinicialização do equipamento de Mitigação ADS para comprovar que não haveria interrupção no tráfego de rede mesmo com a sua total indisponibilidade.

1. Foi realizado comandos de ping da máquina atacante Kali para a vítima (192.168.150.2) que não apresentou nenhuma interrupção.
2. O mesmo comando direcionado a interface de gerência do mitigador ADS (172.16.0.198) que estava operacional até o comando de reinicialização.

Com isso demonstramos a continuidade da conectividade entre a máquina KALI e a vítima sem problemas e o retorno da conexão com a interface de gerência do ADS após a reinicialização.

Evidências disponíveis nos seguintes arquivos:

- [Ping - Antes da Reinicialização do ADS](#)
- [Ping - Depois da Reinicialização do ADS](#)
- [Ping - ADS Restabelecido](#)
- [Evidência Reinicialização do ADS](#)

### Mitigação de Ataques e Filtragem de Tráfego Ilegítimo sem Prejudicar Tráfego Legítimo

*Mitigação de ataques e limpeza do tráfego ilegítimo sem impedir/prejudicar o tráfego legítimo, sejam eles originados de um ou mais endereços IPs, mesmo que esses tenham sido originados através de, por exemplo, um proxy, NAT ou CGNAT.*

**Método Utilizado:** Foi realizado um ataque utilizando o IP de origem da máquina atacante Kali em direção a máquina vítima e em uma outra sessão fechamos um telnet na porta 80 da máquina Kali em direção a máquina vítima. A conexão foi realizada com sucesso, exemplificando que o mitigador bloqueia o tráfego ilegítimo sem impedir/prejudicar o tráfego legítimo.

Evidências disponíveis nos seguintes arquivos:

- [Kali - Ataque Realizado](#)
- [Kali - Acesso Valido Telnet](#)
- [ADS - Tráfego Bloqueado e Tráfego Válido](#)
- [ADS - Logs da Detecção do Ataque](#)

## Mitigação Automática de Ataques com Limitação de Taxa de Tráfego

*O serviço possui suporte à mitigação automática de ataques, utilizando múltiplas técnicas e inclui a Limitação de taxa de tráfego.*

**Método Utilizado:** Neste teste a ideia central é aplicar uma política de limitação de taxa de tráfego no equipamento de mitigação ADS e mostrar em uma máquina atacante como isso se reflete.

1. Foi demonstrado a máquina Kali tentando fazer o download de um arquivo via comando SCP na máquina vítima. No rodapé da tela é mostrada a taxa de transferência que está sempre entre os parâmetros definidos no mitigador.
2. Foram demonstrados os bloqueios gerados pelo tráfego acima do limite definido na política do mitigador, bem como endereço de origem e porta utilizada para tentativa de acesso.
3. O tráfego foi mantido dentro do parâmetro de *rate limit* definido, bem como o tráfego bloqueado por estar acima do limite por segundo definido.
4. Através do parâmetro Group Cleaning Capacity Control foi definido o parâmetro máximo de tráfego para a vítima e todo pacote acima desta taxa será bloqueado.
5. Os pacotes foram recebidos na máquina vítima, demonstrando assim que o tráfego abaixo dos limites definidos é entregue a máquina vítima sem problemas.

Evidências disponíveis nos seguintes arquivos:

- [Comando SCP](#)
- [ADS - Tráfego acima do limite](#)
- [ADS - Parâmetro Rate Limit](#)
- [ADS - Parâmetro Group Cleaning Capacity Control](#)
- [Pacotes recebidos pela Vítima](#)

## Detecção e Mitigação de Ataques DoS/DDoS em IPv4 e IPv6, Incluindo Camada de Aplicação

*O serviço suporta mecanismos capazes de detectar e mitigar todos e quaisquer ataques de DoS e DDoS que façam o uso não autorizado de recursos de rede, tanto para IPv4 como para IPv6, incluindo Ataques à camada de aplicação, incluindo protocolos HTTP, DNS, NTP, SNMP.*

**Método Utilizado:**

1. HTTP - Para o teste foi realizada a geração de tráfego WEB com geração de requisições do tipo GET. Foi demonstrado na Tela do Mitigador NSFOCUS ADS o bloqueio do tráfego HTTP e no Gráfico Attack Traffic o tipo de ataque que foi detectado e a política de mitigação para ataques contra o protocolo HTTP.



2. **DNS** – Para o teste foi demonstrado como é possível efetuar controlos em consultas DNSs realizadas em direção a uma vítima protegida pelo mitigador ADS através de consultas DNS válidas realizada pela máquina Kali em direção a máquina vítima. Nesta consulta foi inserido o domínio baidu.com.br e correios.com.br.
3. **SNMP** - Este teste tem como objetivo evidenciar que o equipamento de mitigação consegue identificar a utilização de parâmetros dentro do payload do pacote SNMP. A ideia central é bloquear consultas de SNMP utilizando a Community public que é padrão para diversos dispositivos e pode trazer problemas ao ambiente do cliente, pois atacantes podem enumerar este serviço e se valer deste parâmetro para obter controle ou informações de um ativo que tenha essa Community e o serviço de SNMP ativo.

- a. Referência da Vulnerabilidade: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0517>

Foi evidenciada a configuração da Community public em forma de expressão regular e a ação de bloqueio caso seja encontrado esta palavra dentro do payload do pacote com a ação de bloqueio como resultado para detecção deste item.

Foram demonstradas as consultas recebidas na máquina vítima com a Community algar, sendo assim, é evidenciado que as consultas estavam disponíveis, porém seguindo os parâmetros definidos na política do mitigador ADS.

4. **NTP** - Este teste tem como objetivo central mostrar de forma prática que o Mitigador ADS pode bloquear ações maliciosas contra a exploração de possíveis vulnerabilidades contra o protocolo NTP.

- a. Referência da vulnerabilidade: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0414>

Foi realizada a captura de pacotes recebidos no mitigador ADS e nela foi possível identificar um padrão nos pacotes utilizados para início do ataque de exploração da vulnerabilidade contra o serviço NTP, sempre existe dentro do payload a string 6stra.

Foi evidenciada a configuração da expressão regular 6stra e a ação de bloqueio caso seja encontrado esta string dentro do payload do pacote com a ação de bloqueio como resultado para detecção deste item.

Evidências disponíveis nos seguintes arquivos:

- **HTTP**
  - [Kali - Ataque ao HTTP](#)
  - [Bloqueio do tráfego HTTP e tipo de ataque detectado](#)
  - [ADS - Política de mitigação HTTP](#)
- **DNS**
  - [Kali - Consulta DNS - baidu.com.br](#)
  - [Kali - Consulta DNS - correios.com.br](#)
  - [ADS - Bloqueio das Consultas DNS - Política DNS keyword Check](#)
  - [ADS - Política de DNS Keyword Checking Ativa](#)
  - [ADS - Bloqueio dos pacotes - Parâmetro baidu.com.br](#)
  - [ADS - Pacote capturado com a consulta DNS para baidu.com.br](#)

- [ADS - Parâmetro que bloqueia a query ao Domínio](#)
- [Payload com a query para o baidu.com.br](#)
- [Payload com a query para o correios.com.br](#)
- [ADS - Pacote capturado com a consulta DNS para correios.com.br](#)
  
- **SNMP**
  - [Kali - Consulta SNMP utilizando a Community public](#)
  - [Kali - Consulta SNMP utilizando a Community Algar](#)
  - [ADS - Bloqueio dos pacotes com a Community public](#)
  - [ADS - Logs do bloqueio através da politica de UDP Regular Expression](#)
  - [ADS - Regra incluída e ativada - UDP Regular Expression Protection - SNMP](#)
  - [ADS - Configuração da Community public e Ação de bloqueio se encontrada palavra no payload](#)
  - [Consultas recebidas na maquina vitima com a Community algar](#)
  
- **NTP**
  - [Kali - tentativa de exploração realizada em direção a Vitima](#)
  - [Kali - Consulta tradicional ao serviço NTP ao mesmo tempo que a maquina Kali](#)
  - [ADS - Bloqueio de Pacotes através da politica de UDP Regular Expression](#)
  - [ADS - Regra incluída e ativada - UDP Regular Expression Protection - NTP](#)
  - [ADS - Padrão nos pacotes utilizados para inicio do ataque](#)
  - [ADS - Padrão nos pacotes utilizados para inicio do ataque 2](#)
  - [ADS - Configuração da 6stra e Ação de bloqueio se encontrada palavra no payload](#)