



---

**Serviço de Gerenciamento de Segurança  
Anti DDoS**

---

### **Anti DDoS Automático**

- Os incidentes de segurança deverão ser tratados pela equipe do Centro de Operações sem que haja necessidade de formalização com o cliente;
- As Alterações de configuração ou perfil do cliente no Anti DDoS Automático poderão ser feitas em acordo com as melhores práticas de segurança;
- O cliente terá acesso aos eventos de ataque por meio do Portal [www.algartelecom.com.br](http://www.algartelecom.com.br);

### **Anti DDoS Manual**

- Os incidentes de segurança deverão ser tratados pela equipe do Centro de Operações e informados à equipe técnica do cliente por meio de contato previamente formalizado;
- As alterações de configuração ou perfil do cliente que contratou o Anti DDoS Manual deverão ser submetidas à avaliação de equipe técnica do cliente e aprovadas por este, sendo o contato por meio telefônico e/ou e-mail.
- O cliente terá acesso aos eventos de ataque por meio de contato telefônico com o Centro de Operações de Segurança da Algar Telecom ou por meio do Portal [www.algartelecom.com.br](http://www.algartelecom.com.br)

### **Visão da especificação técnica**

A solução Anti-DDOS é um mecanismo de defesa que identifica, de forma automática, o comportamento anômalo de serviços em uma rede IP (Ipv4/Ipv6), e possui capacidade de alertar e/ou auto ativar contramedidas para mitigar qualquer atividade maliciosa que se pretenda com ataques de negação de serviço distribuído (DDoS, como definido na sigla em inglês).

A solução integra um sistema de gerência de ameaças que realiza uma inspeção profunda nos pacotes, e permite a redução das ameaças de segurança de maneira rápida e inteligente. Também é eficiente contra quaisquer eventos "desconhecidos" utilizando análise comportamental do tráfego destinado a esgotar a capacidade de banda e/ou dos recursos da rede.

O sistema realiza análises de fluxos de tráfego buscando por padrões de comportamento anômalo que indiquem a presença de ataques do tipo DDoS. Uma vez identificada esta condição anômala, o tráfego pode ser filtrado e então são descartados os pacotes do ataque, permitindo somente a passagem dos pacotes legítimos.

## **Arbor TMS**

Existe um TMS na rede da Algar, que recebe o tráfego da rede quando acionado pelos operadores da solução. O Arbor TMS faz uma análise cirúrgica de cada pacote recebido e remove o conteúdo considerado malicioso de acordo com as configurações aplicadas, deixando fluir apenas o tráfego considerado legítimo até o destino final.

Neste tipo de solução temos três caminhos para o tráfego na rede:

Native path traffic – É o caminho nativo do tráfego da rede, ou seja, caminho pelo qual o tráfego entre origem e destino segue inalterado, resultado da escolha definida pelos protocolos de roteamento;

Off-ramp traffic – É o tráfego desviado do native path para o Arbor TMS, onde este tráfego será analisado.

On-ramp traffic – É o tráfego que é encaminhado de volta para a rede através da interface de saída do Arbor TMS, e deverá seguir até o destino final.

## **Visão lógica**

Em qualquer área crítica de negócio é essencial ter visibilidade, autonomia e eficiência na resposta aos incidentes, determinando assim a sobrevivência em mercados competitivos.

Nossa solução oferece uma plataforma que permite visibilidade ampla sobre tráfego que flui pelo backbone, permitindo criar objetos a serem monitorados e analisar os perfis de comportamento deles.

Estes objetos podem ser clientes, roteadores, circuitos, redes, serviços, protocolos, dentre outros. É possível, então, identificar e alarmar alguma anomalia no comportamento destes objetos até a camada de transporte.

Muito mais que a visibilidade da rede e a identificação de anomalias, esta solução também oferece a possibilidade de rentabilidade através da comercialização de serviços suportados por ela.

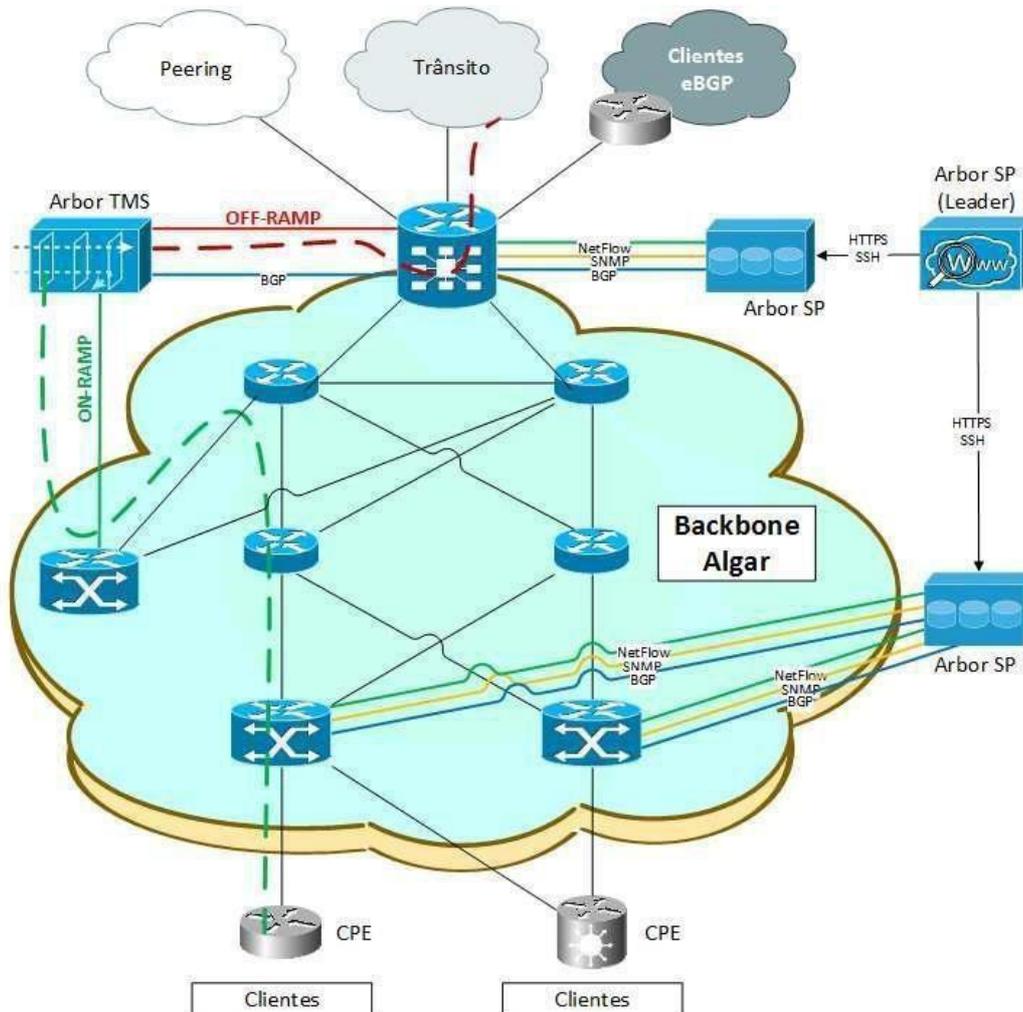
Com os dispositivos de monitoramento podemos entender melhor a origem do tráfego malicioso, seu impacto na infraestrutura, suas características, e utilizar essa informação para obter resoluções efetivas.

Além disso, nossa solução também nos fornece uma visão sobre novas ameaças mundiais e seus perfis de tráfego através do Arbor Networks ATLAS, do Arbor's Security Engineering & Response Team (ASERT), e do Mapa Digital de Ataques. Este último apresenta as ameaças em tempo real, além do histórico desde a sua criação em 2013.

## Arquitetura de Roteamento

A arquitetura em nossa rede dispõe de um único TMS que poderá atrair o tráfego de um ataque e, se for o caso, efetuar o descarte do tráfego malicioso durante uma mitigação.

Na topologia proposta pela Algar, este TMS será conectado ao Peering (borda) e ao Provider Edge (acesso), design que atende aos clientes que estejam conectados na camada da rede onde é feita a reinjeção do tráfego após a limpeza.



## Plataforma

O Arbor Sightline integrado ao Threat Mitigation System (TMS) é uma solução reconhecida líder de mercado em proteção DDoS. Esta plataforma combinada com o nosso SOC é a maneira ideal para enfrentar essas ameaças cada vez mais comuns.

## Inteligência

Aproveitando de uma rede global de monitoramento e sensoriamento, os pesquisadores da Arbor desenvolveram a Atlas Intelligence Feed (AIF), uma biblioteca de defesas automatizadas contra ataques baseado em botnet e neutralização de ameaças emergentes, atualizada constantemente.

## Proteção Contra Ataques

A solução possui contramedidas para vários tipos de vulnerabilidades e fornece proteção para ataques de:



- Reflexão/amplificação (TCP, UDP, ICMP, DNS, mDNS, Memcached, SSDP, NTP, NetBIOS, RIPv1, rpcbind, SNMP, SQL RS, Chargen, L2TP, Microsoft SQL Resolution Service);



- Fragmentação (Teardrop, Targa3, Jolt2, Nестea);



- Pilha TCP (SYN, FIN, RST, ACK, SYN-ACK, URG-PSH, outras combinações de TCP flags, slow TCP);



- Aplicação (HTTP GET/POST floods, slow HTTP, SIP invite floods, DNS, protocolo HTTPS);



- SSL/TLS (Malformed SSL floods, SSL renegotiation, SSL session floods);



- Envenenamento de cache DNS;



- Exaustão de recursos (Slowloris, Pyloris, LOIC, etc.);



- Flash Crowd Protection;



- Protocolos de jogos.

## Detecção De Ataques

A plataforma registra os fluxos do tráfego (traffic flow), dados SNMP e BGP dos nossos roteadores para construir modelos relacionais do tráfego de todo backbone. Estes modelos criam linhas de base (baselines) baseados em limiares (thresholds) e comportamentos. E desvios nesta linha de base, como num ataque de negação de serviço, geram alertas no sistema.

## Tempo De Detecção

É importante ter ciência que diante de um tráfego anômalo, a plataforma só pode disparar um alerta depois de 60 segundos e este tráfego deve exceder o valor médio durante este intervalo.

Por exemplo, se o tráfego de alta severidade for definido em 1 Mbps, é necessário que num intervalo de 60 segundos o tráfego médio seja maior que 1 Mbps, ou seja, a sua somatória deve ser superior a 60 Mb.

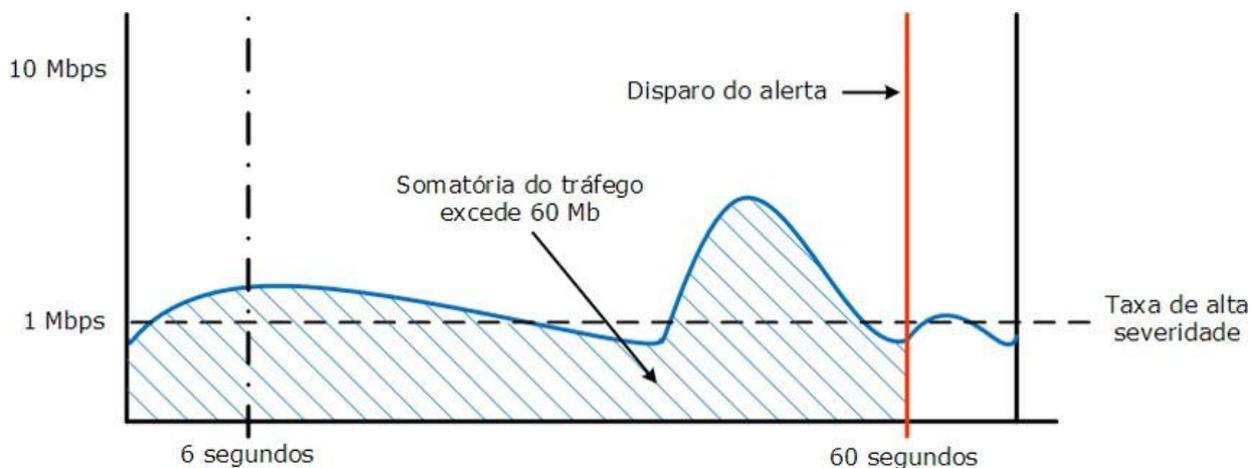


Figura 1 - Tráfego médio alto

O objetivo desta janela de 60 segundos é evitar alertas desnecessários como nos casos de picos de tráfego, como no exemplo abaixo.

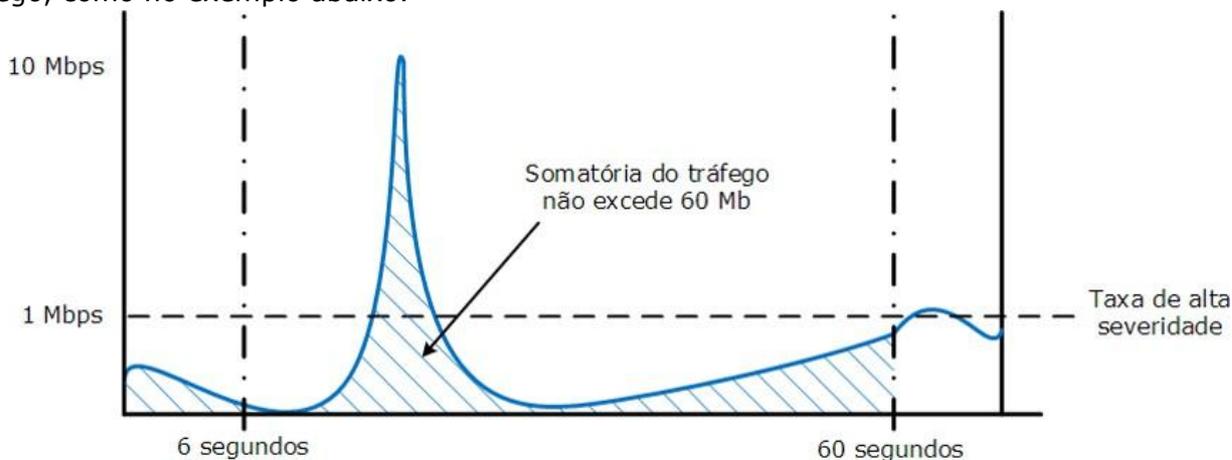


Figura 2 - Pico de tráfego

## Arquitetura De Roteamento

Na solução de Anti-DDoS, os centros de mitigação (TMS) estão conectados aos peering (borda) e aos Provider Edge (PE). Neste tipo de arquitetura, não é necessário a instalação de um hardware em linha (inline) com o seu link, reduzindo os pontos de falha e agilizando a implantação.

Durante uma mitigação, podemos resumir o encaminhamento dos pacotes em 3 (três) fases distintas



**Native path traffic:**  
a rota nativa do tráfego da rede, ou seja, o caminho pelo qual o tráfego entre origem e destino segue inalterado, definidos pelos protocolos de roteamento dinâmico;



**Off-ramp traffic:**  
o tráfego desviado da rota nativa, encaminhado ao centro de mitigação, para tratamento dos pacotes;



**On-ramp traffic:**  
o tráfego que é reinjetado no backbone pelo centro de mitigação para encaminhamento até o destino original.

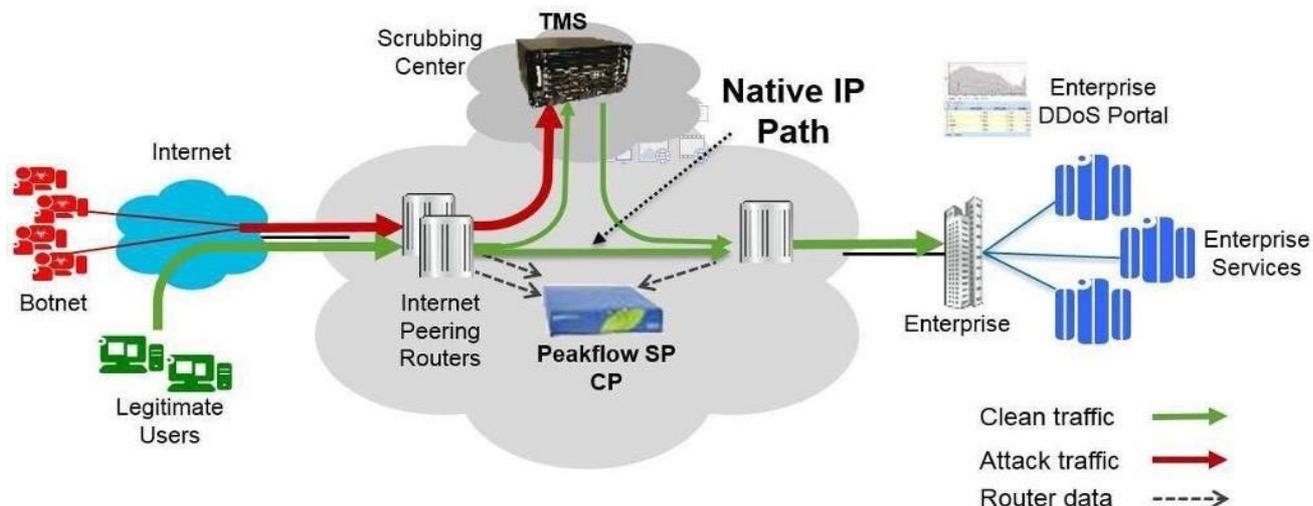


Figura 3 - Arquitetura de roteamento

### Processo De Mitigação

O processo de identificação e mitigação de um ataque de negação de serviço pode ocorrer de formas distintas. No Anti-DDoS não há limitações na quantidade de incidentes e no volume de tráfego mitigado.

Abaixo estão descritos os principais modos de atuação.

### Alerta Da Plataforma

A principal forma de atuação do Anti-DDoS é através dos alertas da plataforma. Por meio deles pode-se desencadear duas ações distintas: automática ou manual. Um destes modos de atuação deve ser escolhido pelo cliente durante o processo de ativação do produto e pode ser alterado posteriormente.

### Mitigação Automática

Após um alerta, a mitigação será iniciada de forma autônoma e, em paralelo, o SOC acompanhará o processo.

Este modo é indicado para clientes que necessitam de um tempo de resposta ao incidente muito rápido.

### Mitigação Manual

Mediante um alerta, o SOC entrará em contato com o cliente para avaliar, conjuntamente, qual o impacto em seu ambiente. Caso um ataque seja confirmado e o cliente aprove, a mitigação será ativada e as contramedidas ajustadas de acordo. Na situação de um falso positivo, os parâmetros de detecção serão ajustados.

Este modo é indicado para clientes que possuam aplicações sensíveis a latência ou customizadas.

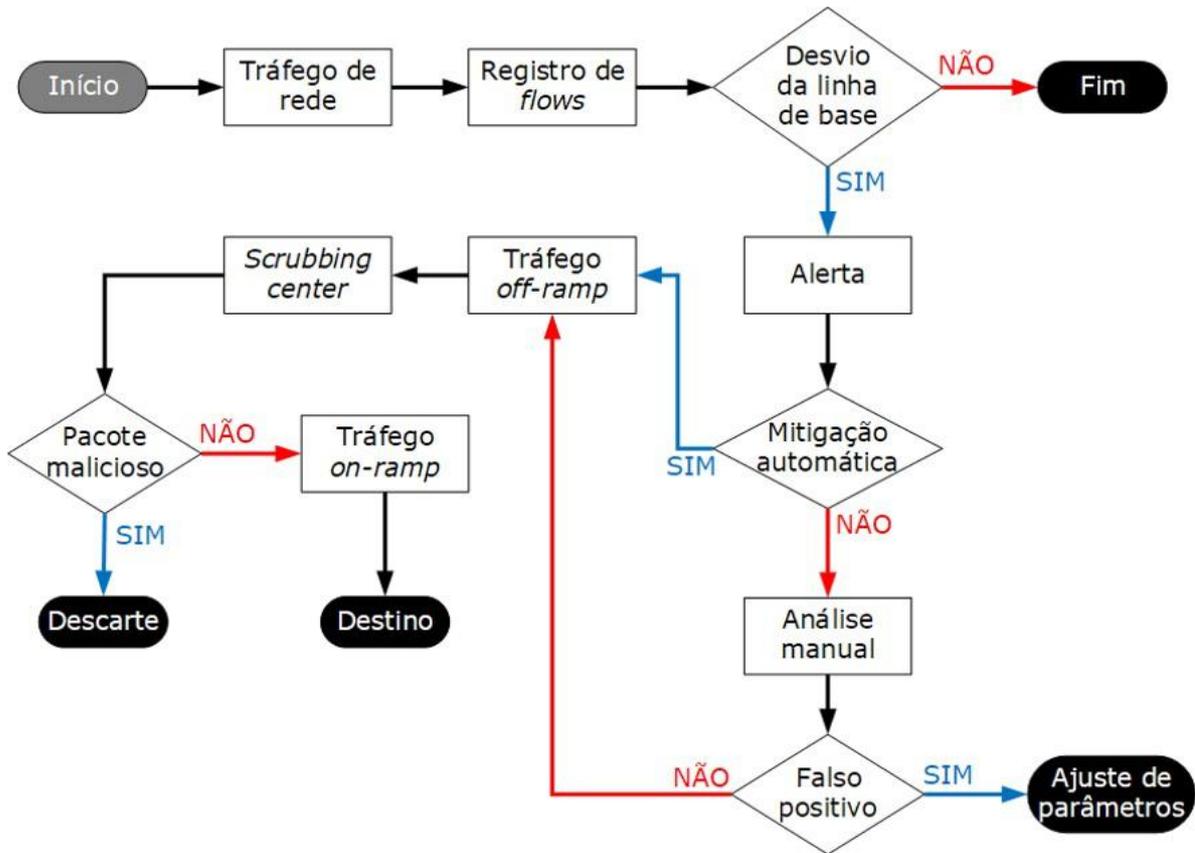


Figura 4 - Fluxograma do alerta

### Contato Do Cliente

Embora a plataforma mantenha o monitoramento constante da rede, a possibilidade de um falso negativo nunca deve ser descartada e, para estes casos, o SOC está disponível para ser acionado pelo cliente. Um analista ao averiguar os indicadores da plataforma pode confirmar ou descartar a existência de um ataque e, posteriormente, realizar os ajustes necessários mediante a confirmação do incidente.

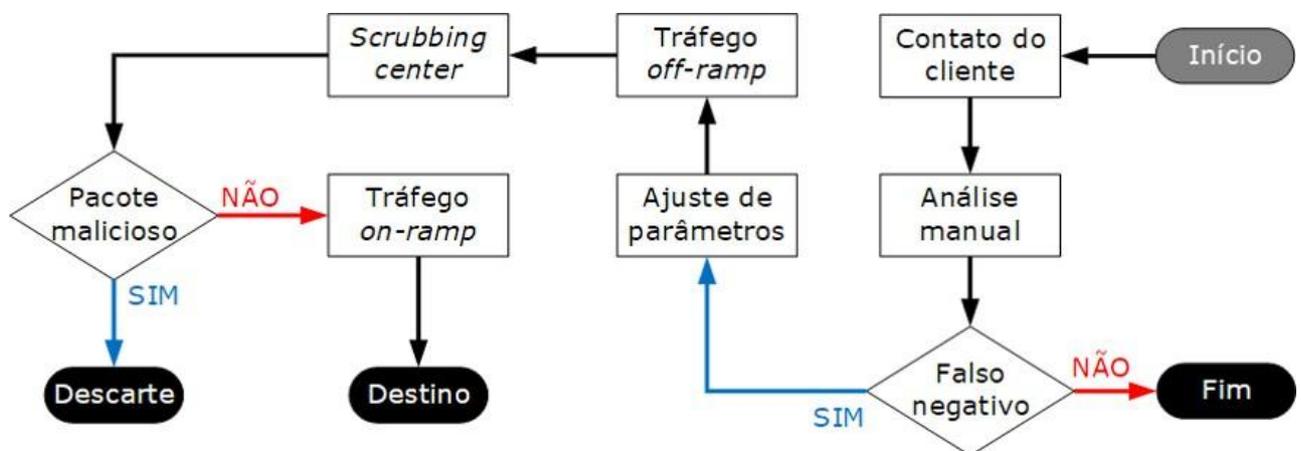


Figura 5 - Fluxograma do contato do cliente

### Blackhole

A blackhole é uma rota anunciada via BGP, distribuída para todos os roteadores do backbone, com a finalidade de dirimir um ataque de negação de serviço.

A sua utilização é uma contramedida adotada nos casos de último recurso como: sobrecarga dos centros de mitigação ou impacto no backbone. Este modo de mitigação, embora indisponibilize o IP anunciado, preservar a infraestrutura de roteamento da operadora e o link de acesso do cliente.

Normalmente, a blackhole é ativada quando o centro de mitigação está comprometido e após a análise do SOC, conforme fluxo abaixo.

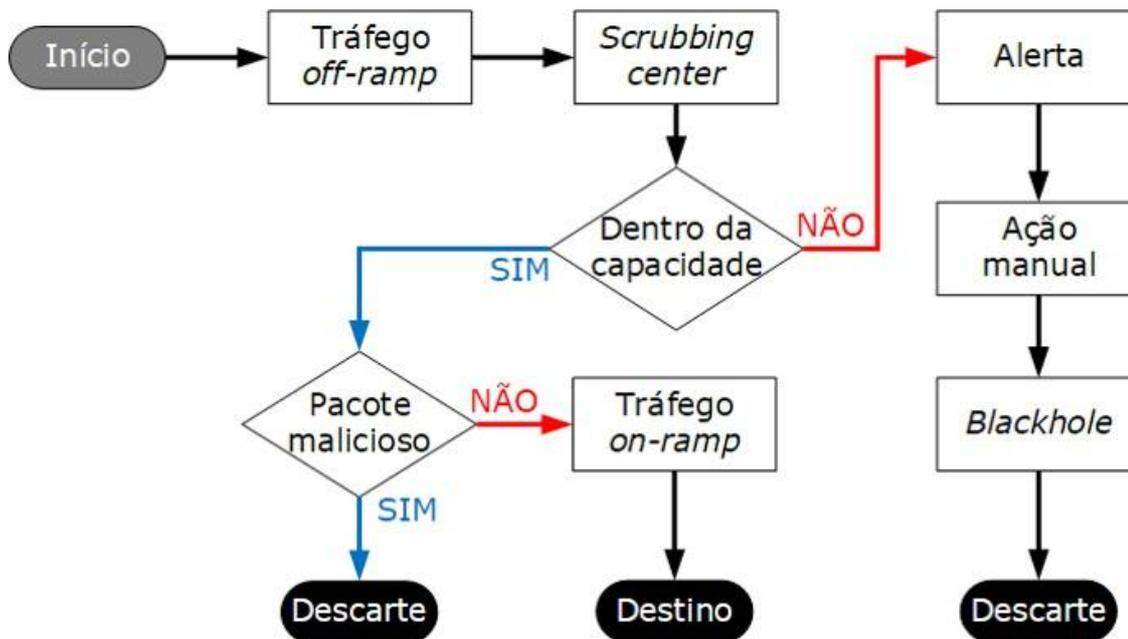


Figura 6 - Mitigação via blackhole

## Portal Do Cliente

Para os clientes que necessitam de uma visibilidade maior e desejam mais detalhamento dos ataques DDoS, pode-se optar pelo atributo Acesso ao Portal.

Na tela inicial, o portal disponibiliza uma visão resumida do seu tráfego e dos alertas classificados por severidades e status, se estão ativos ou não.

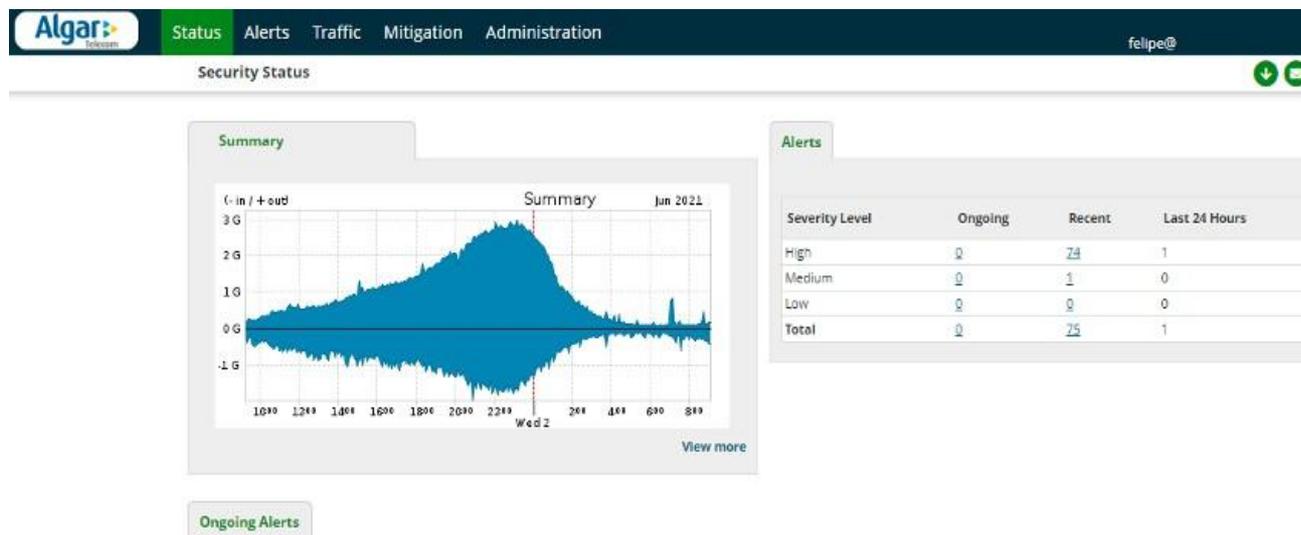


Figura 7 - Tela inicial do portal

A partir do menu Alerts são exibidos todos os alertas contendo o seu número de identificação (ID), a criticidade, endereço IP (detecção por host) e dados gerais do evento como: tipo de ataque, horário de início e duração

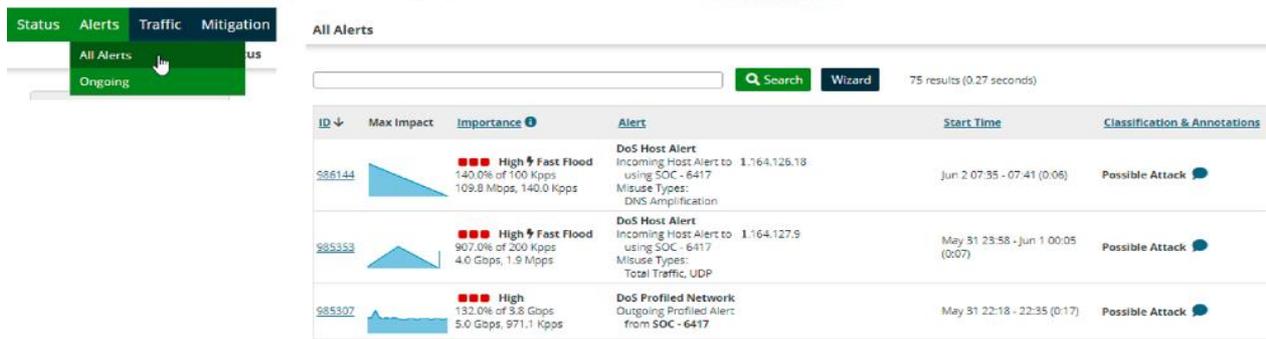


Figura 8 - Alertas

Também é possível obter mais detalhes sobre as características do alerta através da apresentação do gráfico de volumetria, segmentado por tipo de tráfego.

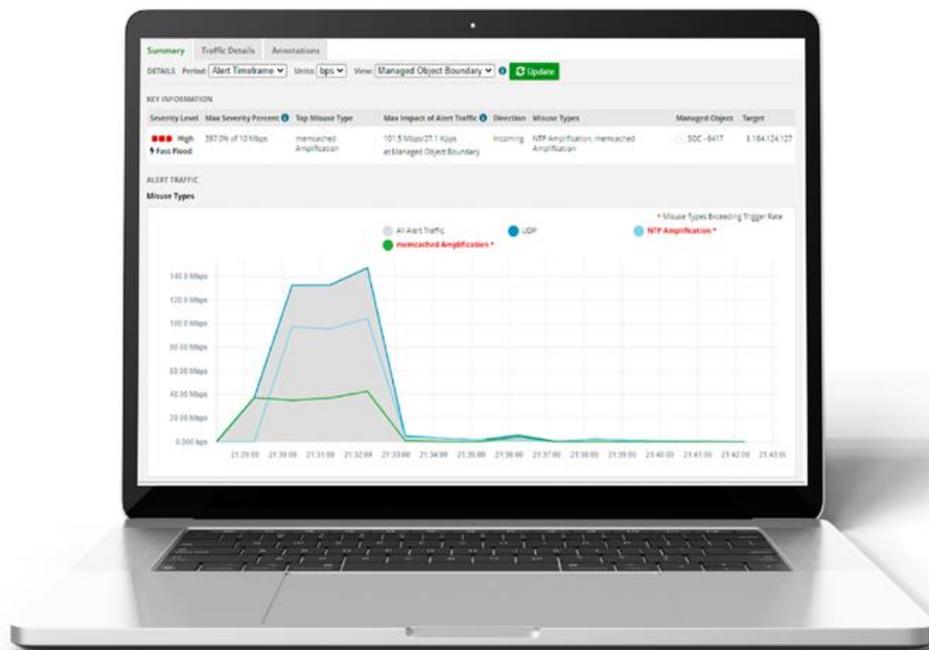


Figura 9 - Gráfico de volumetria

E outras informações técnicas como endereços IP de origem e destino, portas de origem e destino, distribuição do tamanho dos pacotes, etc

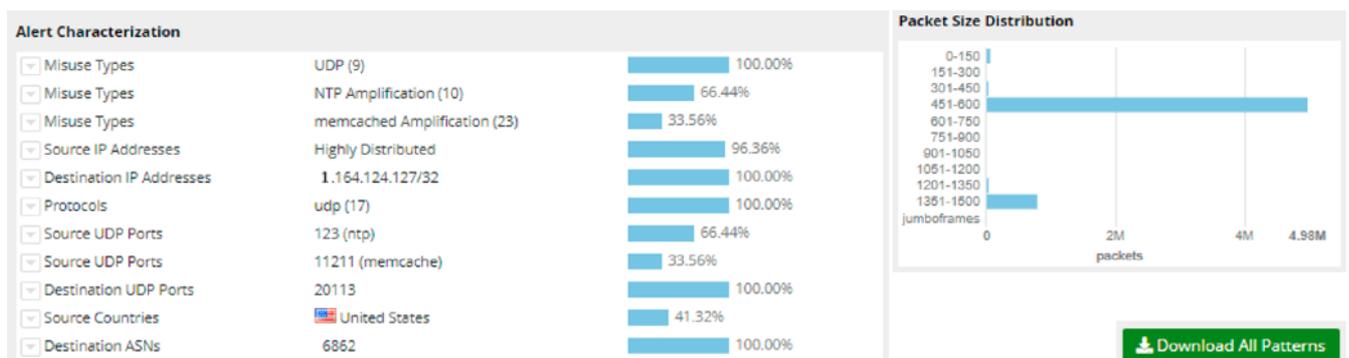


Figura 10 - Características do alerta

Além de todo este conteúdo, o portal disponibiliza outros dados relevantes como quais contramedidas estão aplicadas, o tráfego permitido e descartado durante a mitigação; a lista de aplicações, protocolos, portas e endereços IP com maior utilização de tráfego.

Limite de implantação: até 3 usuários por cliente.

## Detecção Por Host

Normalmente, uma forma de avaliar um ataque de negação de serviço é checar a utilização como um todo do tráfego destinado a interface de rede WAN. Porém, isso não é suficiente para a detecção de ataques de exaustão como o SYN flood, por exemplo, ou alterações no comportamento de um IP específico dentro segmento de rede.

Para resolver este problema, existe a detecção por host. Ela funciona pelo monitoramento do tráfego de cada IP, seja IPv4 ou IPv6, contido no bloco de endereços (CIDR). Ou seja, a alteração no padrão de comportamento de um único IP é suficiente para disparar um alerta.

A plataforma se utiliza de parâmetros pré-definidos para categorizar o tráfego. Estes parâmetros estão listados abaixo e podem ser ajustados de acordo com o perfil de utilização.

Tabela de tráfego anômalo para detecção por host:

Tipo de anomalia	Tipo de Tráfego
Tráfego Total	Tráfego total (bps ou pps) para um determinado host
Amplificação CHARGEN	Tráfego CHARGEN (bps ou pps) no protocolo UDP e porta de origem 19
Amplificação CLDAP	Tráfego CLDAP (bps ou pps) no protocolo UDP e porta de origem 389
DNS	Tráfego DNS (pps) no protocolo TCP/UDP e porta de destino 53
Amplificação DNS	Tráfego DNS (bps ou pps) no protocolo UDP e porta de origem 53
ICMP	Tráfego ICMP (pps). IPv4: tráfego ICMP (protocolo 1) e IPv6: tráfego IPv6-ICMP (protocolo 58).
Fragmentação IP	Fragmentos de pacote não iniciais (pps). Porta de origem e destino 0 (zero) e sem flag TCP.
IP Privado	Tráfego (pps) de endereços IP privados. O Sightline utiliza-se das seguintes sub-redes para detectar anomalias: IPv4 10.0.0.0/8 172.16.0.0/12 192.168.0.0/16 IPv6 Todas as sub-redes exceto 2000::/3
IPv4 Protocolo 0	Tráfego (pps) com número de protocolo 0
L2TP Reflexão/Amplificação	Tráfego de amplificação Layer 2 Tunneling Protocol (bps ou pps) no protocolo UDP, com porta de origem 1701 e com tamanho de pacote entre 500 e 65535 bytes
mDNS Reflexão/Amplificação	Tráfego de amplificação Multicast DNS (bps ou pps) no protocolo UDP e porta de origem 5353
memcached Amplificação	Tráfego memcached (bps ou pps) no protocolo UDP e porta de origem 11211.
MS SQL RS Amplificação	Tráfego UDP (bps ou pps) com porta de origem 1434
NetBIOS Reflexão/Amplificação	Tráfego de amplificação NetBIOS (bps ou pps) no protocolo UDP e porta de origem 137 ou 138
NTP Amplificação	Tráfego NTP (bps ou pps) no protocolo UDP e porta de origem 123. Tamanho de pacotes de 36, 46, 76 e 220 para IPv4, e 56, 66, 96 e 240 para IPv6 estão liberados (whitelisted).
RIPv1	Tráfego de amplificação IPv4 RIPv1 (bps ou pps) no protocolo UDP e porta

Reflexão/Amplificação	de origem 520
rpcbind Reflexão/Amplificação	Tráfego de amplificação rpcbind (bps ou pps) no protocolo UDP e porta de origem 111
SNMP Amplificação	Tráfego SNMP (bps ou pps) no protocolo UDP e porta de origem 161 ou 162
SSDP Amplificação	Tráfego UDP (bps ou pps) com porta de origem 1900
TCP ACK (disabled by default)	Tráfego TCP (bps ou pps) com acknowledge flag ou ambas acknowledge e push flags definidas. Nenhuma outra flag pode ser definida.
TCP Null	Tráfego TCP (pps) que contenha um número de sequência, mas com todas as flags indefinidas
TCP RST	Tráfego TCP (pps) com reset flag. Outras flags podem ser definidas, mas não a flag de sincronização.
TCP SYN	Tráfego TCP (pps) with the synchronize flag set and the acknowledge flag not set. Other flags may be set.
TCP SYN/ACK Amplificação	Tráfego TCP (bps ou pps) com ambas synchronize e acknowledge flags definidas. Nenhuma outra flag pode ser definida.
UDP	Tráfego UDP (pps)

### Contramedidas De Mitigação

As contramedidas são mecanismos de defesa que podem ser usadas para selecionar e remover o tráfego malicioso mantendo, assim, a rede operacional. Diferentes contramedidas são projetadas para impedir diferentes tipos de ataques.

Cada pacote encaminhado para o centro de mitigação passa por um processo de verificação por todas as contramedidas habilitadas. Essas contramedidas podem ser ativas e desativas durante o processo de mitigação e seguem a seguinte ordem de processamento:

Tabela de tráfego anômalo para detecção por host:

Etapa	Contramedidas	IPv4	IPv6
1	Blacklist dinâmica (definida automaticamente por outras contramedidas) Obs.: um pacote deve atender às condições abaixo antes de ser avaliado para inclusão na blacklist. Os pacotes que não atendem a essas condições são descartados: IPv4: O pacote deve conter a parte obrigatória do cabeçalho. A versão IP no cabeçalho deve ser 4. IPv6: O pacote deve conter a parte fixa do cabeçalho. A versão IP no cabeçalho deve ser 6. O endereço de destino deve ser especificado e não apenas zeros.	✓	✓
2	Pacotes Inválidos	✓	✓
3	Lista de filtros de endereços IPv4/IPv6	✓	✓
4	IPv4/IPv6 blacklist/whitelist Filtros em linha (inline) Filtros IPv4/IPv6 blacklist/whitelist Blacklist fingerprints	✓	✓

5	Filtragem de cabeçalho de pacote	✓	✗
6	Lista de filtros de localização IP	✓	
7	Zombie Detection	✓	✓
8	Proteção de reflexão/amplificação UDP	✓	✓
9	Proteção contra flood por conexão	✓	✓
10	TCP autenticação SYN (inclui autenticação HTTP)	✓	✓

Tabela de tráfego anômalo para detecção por host:

Etapa	Contramedidas	IPv4	IPv6
11	<p>DNS scoping O escopo (scoping) não é uma contramedida. Mas é um grupo de configurações avançadas que pode aplicar às seguintes contramedidas:</p> <ul style="list-style-type: none"> <li>DNS autenticação</li> <li>DNS limitação de taxa (rate limiting)</li> <li>DNS limitação de NXDomain (rate limiting) (apenas IPv4)</li> <li>DNS expressão regular</li> </ul> <p>O escopo limita o tráfego DNS que as contramedidas DNS processam. Ele faz isso comparando as consultas DNS de domínios com um conjunto de expressões regulares DNS.</p>	✓	✓
12	DNS autenticação (exceto em modo ativo com DNS scoping)	✓	✓
13	Payload expressão regular	✓	✓
14	Linhas de base (baselines) de protocolos	✓	✗
15	Shaping	✓	✓
16	Política de localização IP	✓	✗
17	TCP reset de conexão (apenas detecção de tráfego)	✓	✗
18	TCP limitação de conexão (rate limiting)	✓	✗
19	DNS malformado (ausência de checagem de payload)	✓	✓
20	DNS limitação de taxa (rate limiting)	✓	✓
21	DNS expressão regular	✓	✓
22	DNS limitação de NXDomain (rate limiting)	✓	✗
23	HTTP malformado	✓	✗
24	<p>HTTP scoping O escopo (scoping) não é uma contramedida. Mas é um grupo de configurações avançadas que pode aplicar às seguintes contramedidas:</p> <ul style="list-style-type: none"> <li>HTTP limitação de taxa (rate limiting)</li> <li>AIF e expressão regular HTTP/URL</li> </ul> <p>O escopo limita o tráfego HTTP que as contramedidas HTTP processam. Ele faz isso comparando domínios URL nas solicitações HTTP com um conjunto de expressões regulares HTTP/URL.</p>	✓	✗
25	HTTP limitação de taxa (rate limiting)	✓	✗
26	AIF e expressão regular HTTP/URL	✓	✗

27	SIP malformado (ausência de checagem de payload)	✓	✗
28	SIP limitação de requisições	✓	✗
29	Negociação TLS	✓	✗

## Manutenção

OS clientes terão tratativa e SLA diferenciados conforme o pacote que estiverem ativos:

Serviço Automático: O cliente deverá usar o Portal para ver os ataques sofridos, bem como as ações que foram executadas.

Toda dúvida ou problema deverá ser direcionada para o SOC pela equipe que atender o cliente.

SLA: 5 minutos

Serviço Manual: atendido sempre pelo SOC, 0800 940 0512, e os clientes deverão ser avisados antes de qualquer adequação.

SOC abre OS para si mesmo, para registrar trabalho

SLA: 15 minutos para acionar – para atendimento do ataque

## Modificação do Serviço

O cliente poderá modificar o Anti DDoS de Automático para Manual e vice-versa.

Não haverá alteração de Avançado para Manual/Automático, o cliente poderá ter os 2 serviços.

Toda alteração de velocidade do link deverá ser comunicada ao SOC, para nova calibragem da plataforma com no mínimo de **48 horas** de antecedência.

## Portal

Nosso time de atendimento do SOC é quem fará a configuração do cliente, bem como qualquer alteração necessária ou tratativa de problemas, para isto eles utilizarão o Portal próprio da Plataforma.

Os clientes também poderão acessar o Portal para avaliar os tipos de ataque e as mitigações realizadas em seus links e exporta-los na forma de relatório, para isto precisará logar no portal [www.algartelecom.com.br](http://www.algartelecom.com.br) com o seu usuário e na página de exibição dos Serviços Contratados escolher o seu link que possua o serviço Anti DDoS.

Segue abaixo um esboço do portal.

Nome e Sobrenome [ Sair ]

SELECIONE SEU PRODUTO

Telefone Fixo (034) 3232 1212

BANNER

Plano: Plano 20 centavos Contrato: G12121212 Vencimento: 03 Ativação: 03/10/2011  
 CNPJ: 12.121.121/0001-12

OS PESSOAIS

FAZENDA

SERVIÇOS

**FATURAS**  
 Consulte suas faturas e datas de vencimento.

**REPARO**  
 Solicite o reparo de serviço.

**SOLICITAÇÕES**  
 Acompanhe todas as suas solicitações.

**NOC**  
 Acompanhe serviços NOC.

**ANTI DDoS**  
 Acompanhe a segurança do seu link

### Resumo das informações – Visão cliente

**customer Summary**

**Alerts**

Severity Level	Ongoing	Recent	Last 24 Hours
High	1	193	1
Medium	0	2	0
Low	0	0	0
<b>Total</b>	<b>1</b>	<b>205</b>	<b>1</b>

**Ongoing Alerts**

ID	Graph	Importance	Alert	Start Time	Classification & Annotations
138684		High	DoS Host Alert. Incoming Host Alert to 200.1.40.40 using ALGAR. Misuse Types: TCP SYN, Total Traffic	Sep 12 10:17 - Ongoing (0:19)	Verified Attack Escalated (by customer)

O cliente poderá clicar no gráfico para obter mais detalhes ( próximo slide)

## Resumo das informações – Visão cliente

Não deveremos apresentar abas que não serão visualizadas e também deverá estar em português ou com opção para seleccionar idioma

Mitigation: None

Severity Level: **High** Severity Percent: 157.0% of 100 pps Impact: 50.2 Kbps / 157 pps Direction: Incoming Misuse Types: TCP SYN, Total Traffic Managed Object: ALGAR Target: 200.1.40.40  
Top Misuse Type: Total Traffic at Managed Object Boundary

Alert Traffic

Top Traffic Patterns (last 5 minutes)

Source	Protocol	Flags	Src Port	Destination	Dest Port	Alert Traffic
1. Highly Distributed	TCP	S	1024 - 65535 (Dynamic)	200.1.40.40/32	80 (www-http)	151.00 pps

Alert Characterization

Misuse Type	Count	Percentage
TCP SYN (9)	9	100.00%
S (Synchronise)	9	100.00%
Total Traffic (7)	7	100.00%
NULL (0)	0	100.00%
Destination TCP Ports	80 (www-http)	96.00%

Packet Size Distribution

Size Range	Percentage
0-150	100.00%
151-300	0.00%
301-450	0.00%
451-600	0.00%
601-750	0.00%
751-900	0.00%
901-1050	0.00%

Ainda não sabemos como a Mitigação será apresentada , mas acredito que será um item logo abaixo como Informações .

Precisaremos avaliar com a PROMON

## **Infraestrutura do Serviço de Gerenciamento de Segurança – Anti DDoS**

Informamos que a infraestrutura de proteção contra-ataques de DoS/DDoS é composta por centros de mitigação distribuídos nacional e internacionalmente conforme abaixo:

### **1. Arbor TMS Appliance HD1000 (nacional)**

- Capacidade de Mitigação: Até 400 Gbps;
- Endereços de Instalação:
  - PIAF: R. Casa do Ator, 415 - Vila Olímpia - 04546-001
  - CENESP: Av. Maria Coelho Aguiar, 215 - Jardim São Luis - CEP 05805-000

### **2. Arbor TMS Appliance HD1000 (nacional)**

- Capacidade de Mitigação: Até 400 Gbps;
- Endereços de Instalação:
  - SP4: Avenida Ceci, 1900, Tamboré Barueri, São Paulo, Brasil, 06460 120
  - CENESP: Av. Maria Coelho Aguiar, 215 - Jardim São Luis - CEP 05805-000

### **3. Arbor TMS Appliance HD1000 (internacional)**

- Capacidade de Mitigação: Até 400 Gbps;
- Endereços de Instalação:
  - Equinix Miami: Miami, 50 NE 9th St FL- OU AS, ZIP: 33132 Equinix Miami
  - Equinix MI3: Boca Raton, 4680 Conference Way South, Suite 150 Boca Raton, FL, 33431 US

Obs.: Todos os equipamentos são suportados por sistemas de proteção contra quedas de energia, contendo quadros elétricos e disjuntores, No-breaks, sistemas de geração de energia, para-raios e DPS.