br.digital TELECOM

Com a gente ao seu lado, **sempre tem solução**.

Anti-DDoS

Arbor Sightline

Anti-DDoS

Arbor Sightline

Mitigação

"Mitigação" tem origem no latim e significa "ato de tornar mais suave, ameno ou menos severo". Assim, "mitigar" significa tornar algo **menos** intenso, **menos** grave ou **menos** doloroso.

Nosso trabalho é **reduzir o dano**. A Internet é uma rede totalmente imprevisível. Da mesma forma que não temos como prevenir quando um desastre vai acontecer e quais os danos, não temos como prevenir ataques DDoS e seus danos.

Assim como um Antivirus não **impede** seu computador de ser contaminado(dano), o Anti-DDoS não impede ataques e eventuais falsos positivos(dano) ou garante SLA de 100%.

br.digital TELECOM

Anti-DDoS

Arbor Sightline

Plataforma

A proteção anti-DDoS (Distributed Denial of Service) da Arbor Sightline é uma solução avançada que ajuda a proteger redes e servidores contra-ataques DDoS, que têm como objetivo sobrecarregar e derrubar sistemas ao enviar grandes volumes de tráfego de rede malicioso.

br.digital TELECOM

Anti-DDoS

Arbor Sightline

Funcionamento

O Arbor Sightline funciona de maneira integrada para detectar, mitigar e responder a ataques DDoS em tempo real, utilizando as seguintes abordagens principais:

- **Detecção de Tráfego Anômalo**: O Arbor Sightline utiliza técnicas de análise de tráfego para monitorar e identificar padrões incomuns que possam indicar a presença de um ataque DDoS. Ele analisa tanto o tráfego de entrada quanto o de saída da rede, comparando-o com comportamentos normais conhecidos. Quando algo fora do comum é detectado, o sistema pode sinalizar esse comportamento como potencialmente malicioso.

br.digital TELECOM

Anti-DDoS

Arbor Sightline

Funcionamento

- **Coleta e Análise de Dados:** O sistema coleta dados detalhados sobre o tráfego da rede e gera relatórios que ajudam na análise forense. Essa coleta é fundamental para detectar ataques DDoS em suas fases iniciais, antes que eles possam causar danos significativos.
- **Mitigação de Ataques:** Quando um ataque é identificado, a Arbor Sightline pode agir automaticamente para mitigar os efeitos do DDoS, bloqueando ou limitando o tráfego malicioso. Isso pode ser feito redirecionando o tráfego para filtros de segurança ou usando técnicas de "rate limiting", que restringem o número de requisições permitidas por unidade de tempo, impedindo que servidores sejam sobrecarregados.

br.digital TELECOM

Anti-DDoS

Arbor Sightline

Funcionamento

- **Escalabilidade e Resiliência:** A solução Arbor Sightline é altamente escalável, o que significa que ela pode lidar com ataques de diferentes magnitudes, desde pequenos incidentes até grandes ataques de negação de serviço. Ela pode ser configurada para operar em diferentes pontos da rede, oferecendo resiliência em caso de falhas em algum ponto específico da infraestrutura.

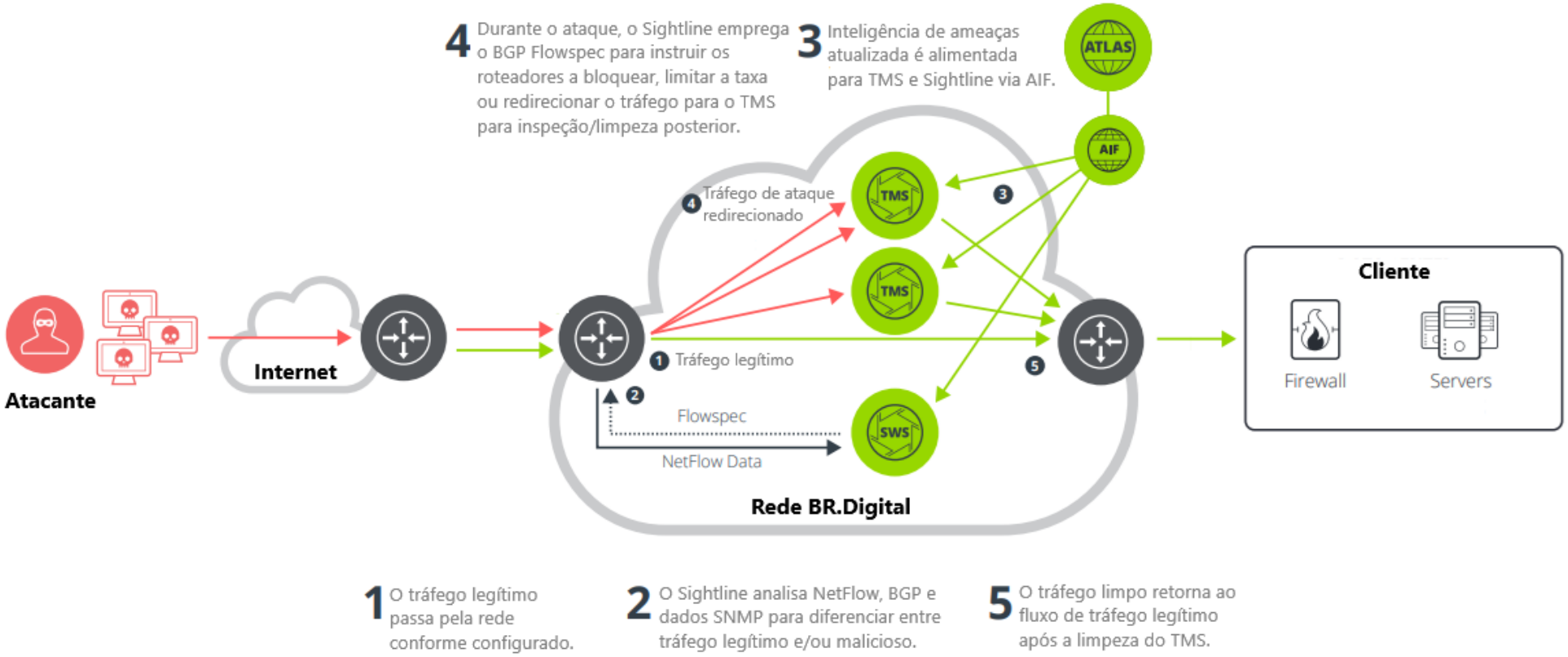
O Arbor Sightline oferece uma proteção robusta contra-ataques DDoS ao combinar detecção inteligente de tráfego anômalo, mitigação em tempo real e escalabilidade, permitindo que as organizações mantenham a continuidade de suas operações sem serem prejudicadas por ataques massivos.

br.digital TELECOM

Anti-DDoS

Arbor Sightline

Topologia



br.digital TELECOM

Anti-DDoS

Arbor Sightline

Modelo OSI

A proteção contra ataques DDoS (Distributed Denial of Service) do **Arbor Sightline** atua em várias camadas do modelo **OSI**, com foco principal nas **camadas 3 (Rede)** e **4 (Transporte)**, onde ocorrem a maioria dos ataques volumétricos. A solução também oferece visibilidade em **camadas superiores**, como a **7 (Aplicação)**, permitindo detectar anomalias e tráfego malicioso com base em comportamento.

br.digital TELECOM

Anti-DDoS

Arbor Sightline

Camada de Aplicação (Layer 7)

A camada de aplicação é onde o tráfego relacionado a serviços específicos da web (HTTP, HTTPS, DNS, etc.) ocorre. Ataques DDoS nesta camada, conhecidos como ataques de camada 7 ou ataques de aplicação, tentam sobrecarregar servidores web ou aplicativos com requisições aparentemente legítimas.

br.digital TELECOM

Anti-DDoS

Arbor Sightline

Camada de Aplicação (Layer 7)

- **Detecção de Tráfego Malicioso:** O Arbor Sightline pode analisar o tráfego HTTP e para identificar padrões anômalos que indicam tentativas de sobrecarga de servidores, como um grande número de requisições HTTP GET ou POST falsas.

- **Mitigação de Ataques a Aplicações:** Quando um ataque é identificado, ele pode usar técnicas como rate limiting (limitação de taxa), que restringem o número de requisições permitidas por segundo de um único cliente, ou challenge-response tests (testes de desafio-resposta) para autenticação do usuário e reduzir falsos positivos.

br.digital TELECOM

Anti-DDoS

Arbor Sightline

Camada de Transporte (Layer 4)

Na camada de transporte, os protocolos mais comuns são o TCP e o UDP. Ataques nesta camada, como os ataques SYN flood ou UDP floods, tentam consumir recursos do servidor ou da rede, como a capacidade de processamento de pacotes ou a largura de banda, com o envio de pacotes falsos ou em grande volume.

br.digital TELECOM

Anti-DDoS

Arbor Sightline

Camada de Transporte (Layer 4)

- **Detecção de Ataques SYN Flood e UDP Floods:** O Arbor Sightline é capaz de identificar picos anormais no tráfego TCP e UDP que indicam tentativas de realizar esses tipos de ataques. No caso de um SYN flood, por exemplo, o sistema pode detectar um alto número de pacotes SYN sem a resposta apropriada, indicando que a rede está sendo sobrecarregada com conexões falsas.
- **Mitigação de Ataques de Tráfego de Transporte:** Após a detecção, o Arbor pode implementar filtragem de pacotes para bloquear pacotes maliciosos ou filtragem de tráfego de porta para evitar que portas vulneráveis sejam sobrecarregadas. Isso inclui o bloqueio de pacotes SYN malformados ou de tráfego UDP de fontes suspeitas.

Anti-DDoS

Arbor Sightline

Camada de Rede (Layer 3)

A camada de rede lida com o roteamento de pacotes entre redes, utilizando o protocolo IP. Ataques DDoS nesta camada, como ICMP floods (ping floods) ou Smurf attacks, são direcionados a sobrecarregar a capacidade de roteadores e redes, causando lentidão ou falhas.

br.digital TELECOM

Anti-DDoS

Arbor Sightline

Camada de Rede (Layer 3)

- **Detecção de ICMP Floods e Outras Anomalias de Tráfego IP:** O Arbor Sightline analisa o tráfego IP em busca de grandes volumes de pacotes ICMP (como em um ping flood), que sobrecarregam a rede com um número elevado de requisições de eco.
- **Filtragem de Pacotes IP Maliciosos:** Quando um ataque IP é detectado, o Arbor pode aplicar filtros para bloquear pacotes ICMP ou pacotes IP maliciosos que estão tentando saturar a rede. Isso pode incluir o bloqueio de pacotes provenientes de IPs falsificados ou desconhecidos, ou a limitação da quantidade de pacotes que podem ser recebidos de uma determinada origem.

Anti-DDoS

Arbor Sightline

Resumo das Camadas de Ação do Arbor Sightline

Em conjunto, o Arbor Sightline oferece uma abordagem de defesa em profundidade, atuando em múltiplas camadas do modelo TCP/IP para identificar, mitigar e bloquear ataques DDoS de forma eficaz e em tempo real.

- **Camada 7 (Aplicação):** Identifica e mitiga ataques que tentam sobrecarregar servidores e serviços específicos (HTTP, DNS etc.) com tráfego malicioso.

- **Camada 4 (Transporte):** Detecta ataques que tentam sobrecarregar a rede com tráfego TCP ou UDP, como SYN floods e UDP floods, e realiza filtragem para evitar esses ataques.

- **Camada 3 (Rede):** Detecta e mitiga ataques que afetam a rede como um todo, como ICMP floods ou Smurf attacks, com filtragem de pacotes IP.

Customer Onboarding Team
cot@br.digital