CONTINENT8 technologies

DDOS

secure8

SECURE | DDOS

Proteção eficaz e escalável contra DDoS

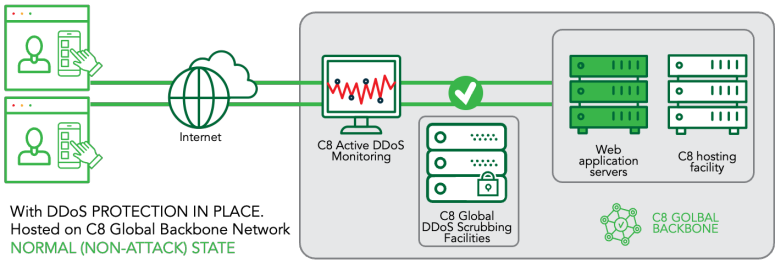
Protegemos as informações mais valiosas do mundo há 25 anos

O serviço de defesa DDoS Continent 8 (C8) é uma plataforma madura e comprovada, construída e desenvolvida ao longo de 18 anos, usando uma combinação de tecnologias e nossa camada customizada de desenvolvimento. Os principais parceiros de tecnologia para nossos ambientes de monitoramento, detecção e mitigação são A10 e Nokia.

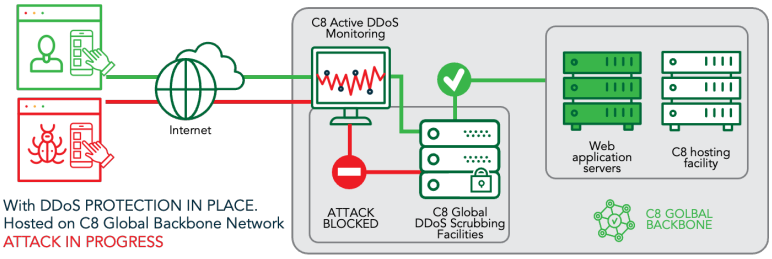
Tempo típico para mitigar um ataque DDoS é de 30 a 60 segundos

Proteção na rede

- A proteção DDOS na rede é para clientes hospedados nos data centers do C8 ou que utilizam a largura de banda IP do C8 em localizações terceirizadas.
- Os clientes podem utilizar os intervalos de endereços IP públicos da C8 ou 'trazer seus próprios' intervalos de provedor independente (sujeito a certos critérios de configuração).
- A mitigação on-net do tráfego DDoS está totalmente sob o controle de C8 e será alcançado por meio de desvio automático usando a injeção de rota BGP e VRFs dedicados.



- O tráfego de entrada é distribuído em torno da borda da rede C8 em um ponto mais próximo da origem.



- Os dados de ataque em tempo real podem ser vistos pelo cliente no Portal C8, onde também podem ser criadas configurações personalizadas de lista de permissões.

- Sob condições de ataque DDoS, o tráfego é desviado para a plataforma de mitigação multi-nós hospedada na rede de backbone global C8. A plataforma seleciona usar o nó de depuração geograficamente mais próximo da origem do ataque.
- Além da depuração, a filtragem de borda de rede pode ser alcançada usando o BGP Flowspec. Isso pode ser implantado com base em informações compartilhadas pelos clientes sobre suas portas e protocolos ativos.

Capacidade agregada de depuração on-net de 1,2 Tbps.

A capacidade total de depuração de 50Tbps+ está disponível através de acordos e sistemas de upstream cuidadosamente projetados.

Arquitetura distribuída global com quatro centros de depuração em localizações geográficas otimizadas.

O tráfego é limpo no ponto de entrada mais próximo usando nossos muitos locais Edge e IX na **Europa:** Londres, Dublin, Paris, Milão, Lisboa, Amsterdã, Marselha, Sófia, **América do Norte:** Nova York, Newark, Los Angeles, Chicago, Dallas, Montreal, Toronto e **Ásia:** Hong Kong, Cingapura, Tóquio.

A10

Nossa plataforma de mitigação A10, que foi integrada de forma otimizada à nossa infraestrutura mais ampla, oferece um conjunto completo de contramedidas de ataque que removem cirurgicamente o tráfego de ataque enquanto mantém o fluxo de tráfego legítimo sem interromper os serviços de rede.

NOKIA

O monitoramento e análise de tráfego Nokia Deepfield oferece visibilidade de rede disseminada e inteligência acionável para que possamos proteger proativamente os serviços de rede dos nossos clientes, melhorar o desempenho da rede e reduzir custos.

GET IN TOUCH
sales@continent8.com

Asia: +65 3165 4649
Europe: +44 1624 694625
Latin America: +54 11 5168 5637
North America: +1 514 461 5120

CONTINENT8.COM/SECURE

FACEBOOK TWITTER LINKEDIN YOUTUBE

CONTINENT8 technologies

DDOS

secure8

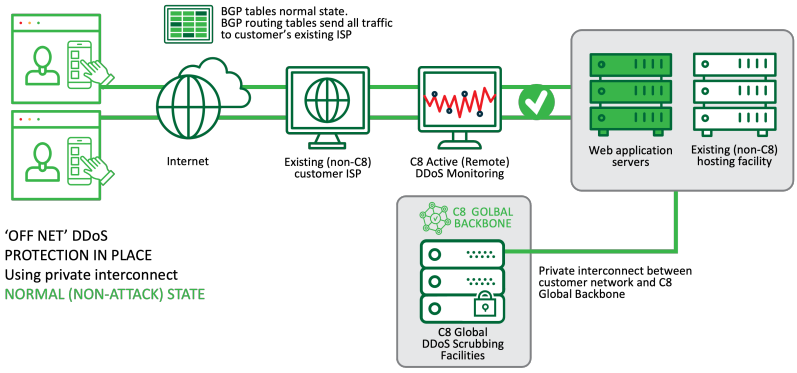
SECURE | DDOS

Proteção fora da rede

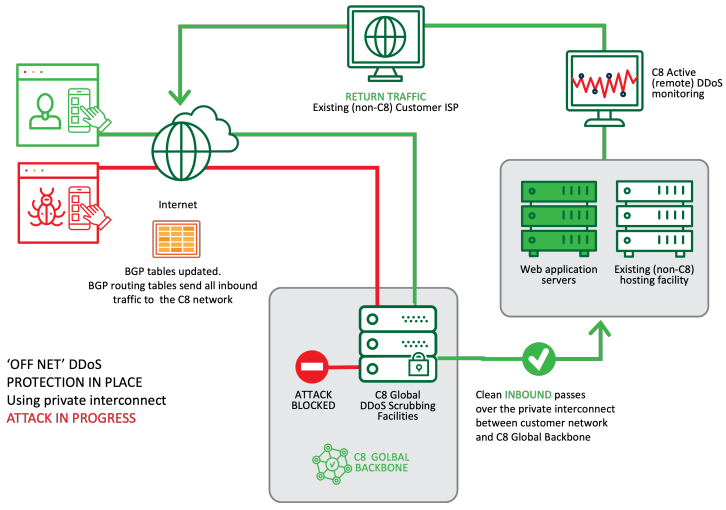
- A proteção off-net está disponível para clientes que não usam a largura de banda IP do C8.
- O tráfego de Internet do cliente pode ser anunciado permanentemente pelo C8 para que o tráfego seja continuamente roteado através da nossa rede para monitoramento eficaz de DDoS e mitigação automática, ou desviado manualmente para o C8 no caso de um ataque DDoS (sujeito à configuração de rede do cliente).
- O C8 pode ajudar no monitoramento remoto de locais para identificar quaisquer ataques e aconselhar quando nossos serviços de mitigação de DDoS são necessários.
- Existem duas opções disponíveis para monitorar e retornar o tráfego para a infraestrutura hospedada do cliente: entrega direta por meio de um circuito privado encapsulado ou usando um túnel GRE pela Internet.

Off-net: Entrega direta usando um circuito privado/Túnel GRE

- Conexão física instalada entre a rede global do C8 e os roteadores de borda da rede do cliente (para resiliência, dois circuitos separados recomendados).
- C8 realizará monitoramento privado e perfilagem do tráfego do cliente, através dos circuitos privados, usando NetFlow, BGP e informações SNMP do equipamento de roteamento do cliente.



- Quando um ataque é detectado em um intervalo de endereços do cliente:
  - O tervalo de endereços será anunciado via BGP em toda a rede global da C8 em vez de com o ISP existente do cliente. (Nota: o clientedeve ter um espaço de endereço IP público mínimo /24 com um provedor independente para assinar este serviço).
  - Todo o tráfego de entrada destinado ao cliente (ambos tráfego de ataque e legítimo) será então encaminhado para a rede C8 e 'limpo', com o tráfego limpo passado para o cliente através do(s) circuito(s) privado(s). (O tráfego de saída ainda será roteado do cliente para a Internet através do seu ISP "normal").
  - Uma opção de Circuito Privado é superior ao uso de um Túnel GRE, pois o trafego do cliente é entregue por uma rede privada em largura de banda dedicada, apoiada por SLA.



TECHNICAL SUPPORT
support@continent8.com

Asia: +65 3165 4796
Europe: +44 1624 694611
Latin America: +54 11 5168 5643
North America: +1 514 461 5111

CONTINENT8.COM/SECURE

FACEBOOK TWITTER LINKEDIN YOUTUBE