Serviços de Proteção DDoS

Global IP Network | Informativo do Serviço

Um Mundo de Insegurança Cibernética

Um número recorde de consumidores entram na Internet para fazer compras, ler notícias e assistir a vídeos, o surgimento de novas e interessantes áreas de negócios, como a Internet das Coisas (IoT) e a virtualização - essas são as tendências que vemos de hoje. Mas um mundo mais conectado também significa mais vias para que criminosos explorem com ataques cibernéticos cada vez mais sofisticados. Empresas e negócios centrados na Internet não podem simplesmente baixar a guarda, pois as falhas de segurança têm o potencial de derrubar redes e causar milhões em prejuízos. Tornar a proteção uma característica essencial ao lançar novos produtos e serviços passa a ser uma obrigação – e uma das preocupações mais críticas no momento.

Ataques DDoS

Entre as principais preocupações nos dias de hoje estão os ataques distribuídos de negação de serviço (DDoS - Distributed Denial of Service), que se tornaram uma ameaça constante à comunidade de negócios na Internet. Eles podem ocorrer a qualquer momento - potencialmente causar efeitos devastadores à sua rede, danificar ativos e gerar grandes perdas de receita. E estes ataques estão crescendo em tamanho, frequência e complexidade - alguns já causaram problemas em centenas de milhares de dispositivos. Eliminá-los antes que eles possam causar sérios danos é, portanto, imprescindível.

Ataques Volumétricos

Os ataques volumétricos são feitos para sobrecarregar uma rede ou host, tornando-o inacessível. Esse tipos de ataques geralmente são originados por dispositivos invadidos ou pela exploração de determinados protocolos de rede, geralmente resultando em algum tipo de dano colateral e tornando a rede inacessível a muitos além do que simplesmente o alvo pretendido.

- **TCP SYN Flood (Inundação TCP SYN)**
- **UDP Flood**
- **ICMP Flood**
- **Ataque por Reflexão**

Ataques à Camada de Aplicação

Ataques à camada de aplicação são ataques muito bem concebidos que visam um serviço específico em um host. Eles podem ser difíceis de se detectar, pois parecem ser uma conexão legítima, mas geralmente são preenchidos com garbage requests (pedidos de lixo). Devido a um grande número de ferramentas disponíveis, como a LOIC, esses ataques tornaram-se ainda mais populares entre os hackers.

- **HTTP-GET**
- **HTTP-POST**
- **Ataques SSL**

Ataques de Exaustão de Estado

Esses ataques podem ser do tipo volumétrico e/ou de camada de aplicação por natureza, muitas vezes gerados por uma ferramenta slowloris de ataques HTTP-GET ou SSL.

Uma Abordagem Proativa para Segurança de Rede

Nós da Global IP Network (Rede IP Global), entendemos completamente a necessidade de se manter a par dessas ameaças cada vez mais complexas. É por isso que adotamos uma abordagem proativa para impedi-las e não uma abordagem reativa depois que o dano já tiver sido feito. Nossos produtos de segurança se destinam ao suporte a ambientes de segurança multiameaça e oferecemos opções personalizadas, permitindo que você escolha o suporte que melhor se adequa à estratégia de defesa cibernética da sua organização.

Nós também ouvimos suas necessidades específicas de segurança para ajudá-lo a fazer a melhor escolha. Você pode ter a certeza de que temos a equipe ideal para suportá-lo: nossa Equipe Dedicada de Segurança de Rede (NST - Network Security Team) tem uma experiência média de mais de 10 anos, provendo conhecimentos realmente aprofundados. Em combinação com a cobertura do nosso backbone IP Global Tier 1, nossa oferta de segurança é inigualável.

Serviços de Proteção DDoS (DPS)

Nossos Serviços de Proteção DDoS (DPS) oferecem uma abordagem abrangente e diferenciada de mitigação DDoS, dependendo do tipo e do nível de proteção desejado. Essas opções possibilitam você escolher a proteção que melhor se adequa à sua estratégia de defesa, caso você queira um nível de suporte básico, intermediário ou alto. E se você necessita de uma proteção forte, nossos serviços têm a capacidade necessária para tratar ataques em grande escala, redirecionando e limpando o tráfego através da nossa plataforma de mitigação. Então, entre em conosco e enfrente os criminosos antes que eles possam derrubar seu serviço.

DPS Control

O DPS Control é o nosso serviço básico. Com esse serviço, os Clientes podem definir listas de controle de acesso (ACLs) permanentes para bloquear a rede contra específicos tipos de tráfego determinados pelo Cliente. Assim, se você não necessita de assistência com mitigação completa, mas ainda quer um serviço robusto no qual você possa realmente confiar para uma proteção básica, essa pode ser a opção certa. Este serviço oferece os seguintes recursos:

Suporte a ACL Permanente

- Suporte a ACL de até 50 linhas
- Suporte a alterações de ACL padrão e emergencial

Acordo de Nível de Serviço (SLA) de Tempo de Resposta para ACL

- SLA de tempo de resposta de 30 minutos para solicitações emergenciais de ACL
- SLA de tempo de resposta de 01 dia útil para solicitações padrão de ACL

DPS Core

Nosso próximo nível de proteção é o DPS Core. Além de oferecer uma variedade de recursos extras, uma camada adicional de garantia é provida pelo suporte de nossa Equipe de Segurança de Rede (NST) – a mesma equipe que defende a Rede IP Global da NTT de ataques. Usando tecnologia de última geração em resposta a uma solicitação de mitigação, nossa equipe pode rapidamente analisar um ataque e adotar as contramedidas necessárias para extinguir o ataque, como identificar os vetores de ataque chaves, filtrar o tráfego e reroteá-lo para nossa plataforma de mitigação para limpeza. Escolha essa opção se quiser uma resposta rápida e eficaz contra atividades maliciosas de DDoS. Além dos recursos básicos do DPS Control, este serviço inclui:

Acesso à Equipe de Segurança de Rede

- Os Clientes DPS Core têm acesso direto à nossa Equipe de Segurança de Rede altamente especializada, para que possam permanecer atualizados durante as mitigações

Acordo de Nível de Serviço (SLA) de Tempo de Resposta de Mitigação

- Tempo de resposta de 15 minutos para solicitações via portal DPS
- 30 minutos para solicitações por e-mail, telefone ou Portal do Cliente

Mitigação de Ataque

- Nossa Equipe de Segurança de Rede emprega uma abordagem de múltiplas camadas e utiliza diversas ferramentas e técnicas, incluindo a limpeza do tráfego de ataque usando nossa plataforma de mitigação

Portal e Relatórios

- Nosso exclusivo Portal DPS fornece acesso a relatórios e ao histórico de mitigações

DPS Detect

Quer um nível de suporte ainda maior e mais completo? O DPS Detect pode ser a resposta. Além dos excelentes recursos oferecidos pelo DPS Core, o DPS Detect adiciona serviços como recursos de detecção que ajudam a notificar os Clientes de ataques potenciais e mitigações iniciadas pelo próprio Cliente com o simples apertar de um botão no Portal DPS. Os Clientes também podem consultar seu histórico de detecções, relatórios de mitigações anteriores e solicitar mudanças de configuração. Portanto, para um serviço de proteção DDoS completo que cobre todos os parâmetros, utilize o DPS Detect. Os recursos abaixo estão incluídos apenas no DPS Detect:

Detecção de Ataque

- Usando limiares definidos pelo Cliente, os Clientes do DPS Detect serão alertados de ataques potenciais através do Portal DPS e, opcionalmente, por e-mail ou syslog

Mitigação Auto-iniciada

- No Portal DPS, os Clientes podem iniciar uma mitigação com base em um alerta de detecção ativo, ou especificando o endereço IP alvo

DPS Max

A oferta mais abrangente de proteção DDoS para Clientes da Rede IP Global é o DPS Max. O serviço usa uma combinação de recursos, conhecimento e estratégias de mitigação da NTT para proteger os Clientes afetados por ataques DDoS, incluindo detecção de ataque e mitigação automática. O serviço é suportado pela nossa Equipe de Segurança de Rede, a mesma equipe que protege a Rede IP Global de ataques.

Mitigação Automática

- Quando notificada sobre um possível ataque DDoS, a plataforma iniciará automaticamente uma mitigação quando o ataque for detectado, rerroteando o tráfego para nossa plataforma de mitigação e interromperá a mitigação quando o ataque finalizar. O Cliente não necessita realizar nenhuma ação.

Para obter mais informações e atualizações sobre a Global IP Network:

Entre em contato conosco: gin@ntt.net
www.gin.ntt.net

Siga-nos no Twitter
@GinNTTnet_Br
@GinNTTnet
#globalipnetwork #AS2914

v042020PTdps