Termo Específico do Produto

Proteção DDoS – Network Security

1. SERVIÇO PROTEÇÃO DDOS

1.1. tecnologia da informação e ataques ddos

Atualmente, a conectividade à Internet é um dos pilares fundamentais utilizado por empresas e organizações em seus negócios. Alguns exemplos destes negócios são:

- ✓ Empresas de serviços (entidades financeiras, empresas do setor turístico, de transporte e logística, lojas online, empresas do setor de TIC, etc.) realizam uma grande quantidade de negócios B2C e/ou B2B através de canais online. Interrupções ou degradações da qualidade desta conectividade geram um impacto direto nas receitas destas empresas, assim como em suas imagens;
- ✓ As entidades públicas estão cada vez mais utilizando o potencial das tecnologias de informação e da Internet para melhorar a prestação de seus serviços aos cidadãos. Muitos dos serviços oferecidos por estas entidades já são prestados através da Internet, tornando esta conectividade um ativo crítico a se proteger;
- ✓ Outras organizações públicas ou privadas que também se comunicam com seu público através de canais online também tem uma grande necessidade de protegê-los, devido à imagem ou por necessidade de manter tais canais sempre disponíveis.
- ✓ Para as operadoras de telecomunicações, a própria conectividade é o bem que gera receita e necessita proteção para evitar indisponibilidades em sua própria rede e de seus Clientes;
- ✓ Para as empresas de tecnologia, que ofertam serviços como os de Hosting e Colocation, é o meio que permite aos usuários finais acessarem as infraestruturas dos seus Clientes hospedadas nos Data Centers, sendo essencial para a prestação dos serviços;

O uso de tecnologias da informação deriva em grandes benefícios para as organizações, mas também inclui certos riscos de segurança, como o uso não adequado (embora não intencional) da tecnologia ou por ações fraudulentas ou com evidente intenção de causar danos e prejuízos.

Entre as inúmeras técnicas utilizadas pelos criminosos atuais, encontram-se os denominados ataques de Negação de Serviço (Denial of Service - DoS) e ataques de Negação de Serviço Distribuídos (Distributed Denial of Service - DDoS). Esses ataques são gerados de diferentes pontos da rede geralmente a partir de botnets, isto é, a partir de computadores previamente comprometidos e controlados remotamente que atuam de maneira coordenada. Seu principal objetivo é tentar evitar a prestação de qualquer serviço causando saturação ou queda de desempenho no link de conexão à Internet, nos servidores que prestam os serviços e nos aplicativos da organização atacada, ou bem aproveitando falhas ou limitações desses elementos.

De uma forma resumida, é possível agrupar os ataques DDoS em 3 tipos::

- ✓ Ataques de volume massivo: aqueles que saturam a conexão entre a rede do **CLIENTE** e o ISP. Este tipo de ataque não pode ser solucionado pelo próprio **CLIENTE** e sempre demanda a intervenção da **Vivo Empresas** em sua função de ISP.
- ✓ Ataques do tipo exaustão de recursos: aqueles que saturam a capacidade de conexões dos servidores ou os limites de sessões simultâneas nos Firewalls, balanceadores ou IPS.
- ✓ Ataques de nível de aplicação: Aqueles que utilizando petições legítimas saturam os recursos dos servidores aproveitando falhas no desenho da aplicação ou abusando de operações intensivas em recursos.

As motivações desses ataques podem ser econômicas (extorsão, prejudicar a concorrência, etc.), até políticas ou ideológicas, e tem efeitos negativos nas receitas das empresas em função do lucro cessante, da interrupção que representa em suas operações ou em perdas indiretas por imagem, reputação, confiança e satisfação de seus clientes.

1.2. Sobre o serviço

Ciente da problemática que representa essa ameaça para as organizações, a **Vivo Empresas** implementou em sua própria rede uma tecnologia contra ataques DDoS que permite proteger seus ativos de rede e os de seus Clientes. Por possuir uma posição de líder global em serviços de telecomunicações, a **Vivo Empresas** projetou o serviço **Proteção DDoS** baseado em três centros de mitigação localizados na Espanha, EUA e Brasil. Assim, é possível garantir ao **CLIENTE** as melhores práticas de mercado, combinando a flexibilidade de uma solução local com a robustez de uma operadora global.

O Serviço Proteção DDoS da **Vivo Empresas** tem como objetivo detectar e mitigar ataques DoS e DDoS em pontos estratégicos de seu backbone de rede antes que atinjam a rede do **CLIENTE**.

Uma vez identificado o ataque dirigido a um determinado **CLIENTE**, todo o tráfego é desviado para os centros de mitigação, onde é submetido a diferentes filtros e análises que são capazes de diferenciar o tráfego malicioso do tráfego legítimo, sendo o primeiro descartado enquanto que o identificado como legítimo é redirecionado para a rede do **CLIENTE**. No Brasil, essa mitigação é feita no backbone de **Vivo Empresas** Brasil, minimizando a latência introduzida no tráfego. O serviço se presta unicamente nas redes de comunicações de **Vivo Empresas** e sem necessidade de instalação de hardware no site do **CLIENTE**.

O serviço Proteção DDoS conta com centros de mitigação redundantes, instalados em São Paulo (Ibirapuera e Consolação). Desta forma o sistema é capaz de mitigar os ataques o mais próximo possível do ponto de origem, preservando o link do **CLIENTE** e assegurando sua disponibilidade.

1.3. Beneficios ao CLIENTE

O serviço Proteção-DDoS tem como objetivo fornecer uma solução abrangente de segurança que proteja e possibilite a evolução dos negócios atuais e futuros dos Clientes, baseando-se nos processos, pessoas e tecnologias do SOC da **Vivo Empresas**.

A solução Anti-DDOS da **Vivo Empresas** apresenta as seguintes vantagens:

- ✓ **Solução não intrusiva**: como a instalação acontece na própria rede da **Vivo Empresas**, a mesma não necessita de alterações na rede do **CLIENTE**;
- ✓ **Diferencia o tráfego malicioso do legítimo**: se comparada a outras soluções do mercado que descartam todo o tráfego (legítimo e malicioso) em caso de ataque, o serviço Proteção DDoS da **Vivo Empresas** é capaz de limpar o tráfego permitindo a passagem daquele legítimo;
- ✓ **Preserva a conectividade**: preserva a conexão de Internet e impede que tráfego malicioso interrompa ativos críticos para os negócios do **CLIENTE**;
- ✓ **Mínima latência**: O desvio de tráfego para sua mitigação é realizado dentro da rede local da **Vivo Empresas**, minimizando a latência introduzida pela solução;
- ✓ **Disponibilidade**: a solução da Vivo Empresas é redundante, sem custos adicionais para o **CLIENTE**;

- ✓ **A resposta mais adequada**: a Operadora é a única capaz de oferecer uma resposta para ataques de volumetria que podem saturar qualquer elemento da rede do **CLIENTE**. Por esse motivo, uma correta solução contra ataques DDoS deve ser integrada à rede da operadora.
- ✓ **Conhecimento Global**: o serviço Proteção DDoS da **Vivo Empresas** é prestado em vários países e permite um intercâmbio de informação e melhores práticas entre os ISPs do Grupo.
- ✓ **Relatórios dos ataques**: após cada mitigação o **CLIENTE** receberá relatórios específicos com uma análise dos eventos.

2. Escopo de Fornecimento proteção ddos

O serviço é composto por quatros processos.

2.1. MONITORAMENTO

A primeira característica do serviço é o monitoramento de tráfego dos Clientes. Utilizando equipamentos que analisam o tráfego do backbone IP da **Vivo Empresas** através da coleta de estatísticas por Netflow/cflowd dos seus roteadores, o serviço caracteriza-se pela não necessidade da instalação de equipamentos na rede **CLIENTE** ou de desvio de todo o tráfego para um centro de análise quando não existe ataque em andamento. Além disso, visando proteger a confidencialidade das comunicações dos Clientes, esta monitoração é passiva e não intrusiva, pois analisa unicamente informações estatísticas do tráfego e não seu conteúdo.

Esta funcionalidade do serviço não introduz nenhum ponto de falha adicional na infraestrutura do **CLIENTE**, assim como não afeta a disponibilidade de seus serviços de conectividade. Em caso de falhas na infraestrutura de monitoração, o único ponto afetado será a capacidade de detectar ataques DDoS.

Os ataques DDoS distribuídos são gerados a partir de vários pontos geográficos da Internet, podendo ser de vários países diferentes ou de dentro do mesmo país, apesar do primeiro cenário ser o mais frequente. Considerando isto, a monitoração é realizada utilizando as seguintes estratégias:

- Nacionalmente, nos pontos de acesso da rede em que o tráfego é entregue ao **CLIENTE**;
- Nacionalmente, nos pontos de interconexão da rede IP de trânsito nacional, possibilitando a detecção de ataques nacionais e internacionais provenientes de outras operadoras que estejam direcionados para rede da **Vivo Empresas**;

- Nas conexões com backbone internacional, visando a detecção dos ataques iniciados em vários países de forma coordenada;
- Esta estratégia e modelo de monitoração somente permite que o serviço seja ofertado para Clientes que possuam conectividade internet através do serviço IP Internet da Vivo Empresas, e não de outros provedores. Consequentemente, para Clientes multi-homed, isto é, conectados a dois ou mais provedores, o serviço somente poderá ser oferecido para as conexões IP Internet da **Vivo Empresas.**

2.2. Detecção

A mitigação de ataques pode ocorrer após o processo de detecção pró-ativa realizado automaticamente pela plataforma do serviço ou após notificação pelo CLIENTE:

2.2.1. Detecção Pró-ativa

No caso em que a Vivo Empresas detecte um possível ataque com destino aos blocos de rede do **CLIENTE**, ela contatará aos responsáveis designados pelo **CLIENTE**, para verificar a condição de ataque, avaliar conjuntamente a informação disponível e solicitar autorização parar iniciar o processo de mitigação.

Esta detecção é realizada automaticamente pela plataforma quando há a identificação de anomalia de tráfego com base em dois processos de detecção do perfil do tráfego dos serviços monitorados:

- Baseline: nos primeiros 15 dias de monitoramento do serivço a plataforma identificará o perfil habitual de tráfego do CLIENTE que avalia, entre outros indicadores, a quantidade de pacotes por segundo e/ou em bits por segundo;
- Template de monitoração: são os indicadores máximos (thresholds) para geração de alertas definidos pelo CLIENTE e configurados na plataforma pelo SOC Vivo Empresas.

Para otimizar o processo de detecção pró-ativa de ataques, o CLIENTE deve manter o SOC Vivo Empresas atualizado sobre quaisquer alterações em sua rede, seja na lista de blocos IP monitorados, serviços anunciados ou no perfil de uso da banda do link monitorado. Em caso de alterações no monitoramento do serviço, é necessário um prazo mínimo de 15 dias para que a plataforma possa atualizar o perfil habitual de tráfego do CLIENTE (baseline) e garantir a precisão nos processos de detecção e de mitigação de ataques. Em caso de alteração do perfil do tráfego do cliente sem aviso prévio pelo Cliente ao SOC Vivo Empresas, seja por conta de uma campanha, alteraçao de blocos de redes ou serviços monitorados, não será possível garantir a eficiência nos processos de detecção e de mitigação.

O serviço é capaz de detectar e mitigar ataques com tráfego criptografado cujos pacotes não estão em conformidade com a RFC dos protocolos (abuso de protocolo).

2.2.2. Detecção Reativa

No caso que o **CLIENTE** detecte uma anormalidade no comportamentodos seus blocos IP monitorados, utilizando-se de seus próprios sistemas, deverá contatar a Vivo Empresas para solicitar a análise e, se necessário, iniciar um processo de mitigação. Somente os contatos autorizados pelo **CLIENTE** poderão informar à Vivo Empresas a suspeita de um ataque e ativar a mitigação.

Uma vez estabelecido o contato, o SOC de Clientes de Vivo Empresas e o **CLIENTE** avaliarão conjuntamente a informação disponível e, em caso de confirmar o ataque, a Vivo Empresas solicitará autorização para iniciar a mitigação.

O serviço Proteção DDoS, através da coleta de dados estatísticos dos roteadores do backone IP da Vivo Empresas, oferece unicamente a detecção Proativa de ataques volumétricos, sejam eles massivos ou de exaustação de recursos. Não poderão ser detectados aqueles ataques que não provoquem variações significativas no seu perfil habitual de tráfego (baseline) em quantidade de bits ou pacotes por segundo, e/ou que não atinjam os *thresholds* definidos pelo CLIENTE com o apoio do SOC Vivo Empresas para geração de alertas e/ou aqueles no qual o componente malicioso esteja incluso no payload dos pacotes. Nestes casos, é requerida a colaboração do **CLIENTE** para detectar os possíveis ataques e contatar a Vivo Empresas para coordenar as ações necessárias para a mitigação (Detecção Reativa).

A detecção automática dos ataques de nível de aplicação ou com baixo volume de bits ou pacotes por segundo, assim como para a análise e mitigação de ataques com tráfego criptografado cujo conteúdo malicioso esteja contido no payload dos pacotes, requerem soluções específicas para este fim pois geralmente exigem o monitoramento e análise de todo o tráfego e não apenas estatístico. Esse tipo de escopo é atendido por meio da instalação de softwares e/ou equipamentos adicionais na infraestrutura do **CLIENTE**, o que não será parte da oferta padrão deste serviço.

Os alarmes são registrados no sistema de trouble ticketing para sua consequente avaliação por parte do SOC Vivo Empresas. O serviço tem a capacidade de oferecer a mitigação efetiva de ataques DDoS que se utilizam de tráfego não criptografado.

Os alarmes gerados são avaliados pelos analistas do SOC. Levando em consideração aqueles que são qualificados com severidade Alta e Média, os analistas verificam se realmente existe um ataque em curso. Quando a avaliação é positiva, o SOC entra em contato o **CLIENTE**.

Antes dos períodos indicados acima como necessários para criação ou alteração do perfil habitual de tráfego não é garantida a eficiência dos processos de detecção e de mitigação.

2.3. MITIGAÇÃO

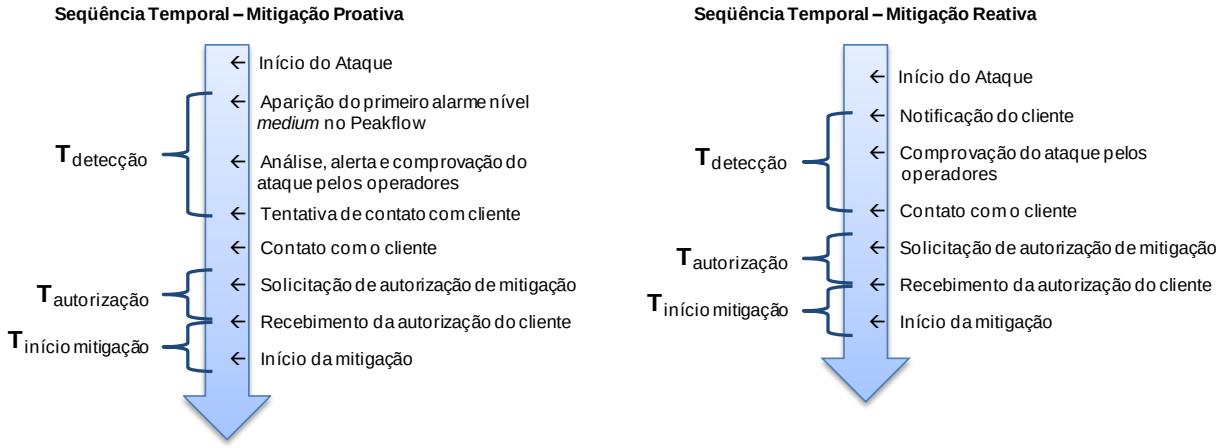
O processo de mitigação inicia-se somente após a autorização explícita do **CLIENTE**. Além de reduzir os efeitos negativos do ataque (indisponibilidade da conectividade ou de algum serviço), a tecnologia utilizada e o modelo de operação do serviço dispõem de capacidade para garantir um tempo de reação máximo. Este tempo se divide da seguinte maneira:

- $T_{detecção}$:
    - **Detecção proativa**: o tempo que transcorre desde que se gera o primeiro alerta do nível medium associado a um ataque até que o SOC avalie a incidência como possível ataque e tente comunicar com o **CLIENTE**;
    - **Detecção Reativa**: o tempo que transcorre desde que o **CLIENTE** comunica ao Service Desk do serviço que está vivendo uma anomalia que considera como ataque DDoS até que a equipe do SOC analise a situação, verifique que se trata de um ataque e o entre em contato com o **CLIENTE**;

$T_{autorização}$: tempo necessário para o **CLIENTE** autorizar a mitigação do ataque, desde solicitação até sua autorização;

O SOC se encarrega de realizar uma análise detalhada do alarme identificando as características do ataque e quais as contramedidas que deverão ser utilizadas. Apóso início da mitigação for iniciada, é realizada uma nova análise do efeito da mesma. Nesse momento, ajustes mais finos podem ser feitos ou novas contramedidas podem ser ativadas caso seja necessário.

É importante destacar que o atacante, quando detectar que o Serviço Web do **CLIENTE** foi recuperado, tentará alterar a técnica de ataque, portanto o SOC e o **CLIENTE** deverão seguir em contato para verificar se a mitigação continua sendo efetiva até o final do ataque.



Mitigação - Sequência Temporal

Destes tempos, o definido como $T_{autorização}$ depende do **CLIENTE**. Assim, o mesmo não é considerado como medida de qualidade do serviço. Estão sujeitos a acordos de serviço os tempos: T-detecção;

Segundo a modalidade comercial contratada pelo **CLIENTE** se empregará uma ou, se necessário, uma combinação das técnicas de mitigação disponíveis no serviço.

Ainda dentro do contexto da mitigação, estão contemplados os seguintes conceitos:

- **Janela de mitigação**: duração máxima de mitigação antes de ser contabilizada uma nova mitigação. .
- **Desativação da mitigação**: tempo máximo para que o SOC Vivo Empresas desative o desvio de tráfego para as plataformas de mitigação após o término de um ataque.
- **Intervalo entre mitigações**: tempo máximo entre uma mitigação e outra antes de ser contabilizada uma nova mitigação.

2.3.1. Mitigação Inteligente

Uma vez que se confirme o ataque e que o **CLIENTE** autorize, será ativado o processo de mitigação. O processo consiste em:

Desviar os fluxos de tráfego direcionado para os blocos de rede alvos do ataque para as plataformas de mitigação;

Identificar o tráfego de ataque e descartá-lo, permitindo que o tráfego legítimo flua normalmente para a rede do cliente;

Entregar o tráfego legítimo ao seu destino final.

2.3.2. Comunicação durante o processo de mitigação:

- O SOC manterá o contato com o **CLIENTE** para informar sobre o ataque e o estado da mitigação.
- Caso seja necessário se poderá estabelecer uma comunicação de áudio direta junto ao **CLIENTE** para melhor resolução do problema.
- A Vivo Empresas notificará ao **CLIENTE** cada vez que se detectem mudanças significativas no perfil do ataque e/ou nas contramedidas de mitigação adotadas.
- O ataque é considerado encerrado quando não houver mais identificação de tráfego ilícito pelas plataformas de mitigação. Após o encerramento do ataque a Vivo Empresas poderá manter o tráfego desviado para as plataformas de mitigação por um período máximo de até 2 horas. O SOC Vivo Empresas informará previamente ao CLIENTE sobre desativação da mitigação.

Em caso de comprometimento da infraestrutura de Vivo Empresas devido a ataques simultâneos aos Clientes do serviço **Vivo Proteção DDoS**, a prioridade de mitigação será a Vivo Empresas, visando sempre manter a infraestrutura de serviços disponível, proporcionando qualidade aos serviços prestados aos Clientes.

2.3.3. Reinserção do tráfego

Para que o serviço seja completamente transparente para os Clientes, o desvio e a reinserção do tráfego são realizados por meio de anúncio BPG/32 que se propaga dentro do backbone IP da Vivo Empresas. Essa técnica permite o encaminhamento do tráfego dos blocos de rede atacados para as plataformas de mitigação e a devolução do tráfego limpo para a rede do CLIENTE.

2.3.4. Finalização da Mitigação

A mitigação será interrompida a qualquer momento, mediante solicitação do **CLIENTE** ou após decorridas 2 horas do encerramento do ataque.

2.4. RELATÓRIOS

2.4.1. Relatório de Ataque Mitigado

Uma vez finalizada a mitigação, o SOC Vivo Empresas disponibilizará um relatório sobre o volume e as características do ataque, sua evolução e as medidas tomadas para mitigá-lo,contemplandoas seguintes informações:

- ✓ Tempo de início e fim do ataque, conforme registrado na ferramenta (mitigação proativa) ou notificado pelo **CLIENTE** (mitigação reativa);
- ✓ Tempo de início e fim da mitigação. Número de mitigações consumidas (para ataques com mitigação ativada por mais de 12 horas);
- ✓ Tipo do ataque e sua evolução (considerando que os atacantes tenham utilizado várias técnicas durante o ataque);
- ✓ Gráfico com a evolução temporal do tráfego dos ataques desde seu início até seu fim;
- ✓ Tempo de ativação de cada contramedida e respectiva avaliação de sua efetividade até a resolução definitiva do incidente;
- ✓ Informações sobre o SLO do serviço (detecção e mitigação);

- ✓ Tipo de detecção: proativa (Vivo Empresas) ou reativa (**CLIENTE**).

Os relatórios de ataque mitigado serão disponibilizados manualmente ao **CLIENTE** pelo SOC de Clientes (através de email).

2.4.2. Relatório de Tráfego

A monitoração do tráfego do **CLIENTE** também pode oferecer informações de valor ao **CLIENTE**, independentemente se houve ou não ataques no período em questão. As seguintes informações são disponibilizadas:

- ✓ Estatísticas sobre o volume de tráfego dividido por aplicação (especificada através de protocolo e porta);
- ✓ Estatísticas sobre a distribuição das subredes IP ou dos sistemas autônomos (AS) a que se enviam e recebem maior volume tráfego;
- ✓ Distribuição dos países que geram maior volume de tráfego para **CLIENTE**;

Estes relatórios agregam um valor adicional ao serviço, principalmente aos Clientes que não são alvos frequentes de ataques, pois confirmaria como o serviço está sempre em execução e protegendo suas redes.

Os relatórios de tráfego serão disponibilizados manualmente ao **CLIENTE** pelo SOC de Clientes (através de email) em intervalos de tempos regulares, conforme plano contratado.

2.4.3. CONFIGURAÇÃO INICIAL

O processo de ativação do serviço consiste nas seguintes etapas:

- Configuração da exportação dos flows dos roteadores da rede IP da Vivo Empresas que proveem acesso internet ao CLIENTE para as plataformas de monitoração.
- Configuração do template de monitoração dos blocos de rede do CLIENTE que fazem parte do escopo de contratação desta proposta. Para que o processo de detecção ocorra de forma adequada é necessário que o **CLIENTE** mantenha o SOC Telefônica|Vivo atualizado sobre as características dos serviços a serem monitorados, particularidades de componentes de sua infraestrutura de rede e de segurança interna assim como seus respectivos limiares de uso adequado. Tais informações serão confidenciais e não poderão ser divulgadas pela **Telefônica|Vivo**.
- Dentro do processo de criação do template de monitoração, será ativado o baseline da rede do CLIENTE, que consiste na monitoração do tráfego do CLIENTE para que aconteça a identificação automática, pelas platataformas de monitoração, do perfil habitual do tráfego do CLIENTE. É necessário que o tráfego seja monitorado por pelo menos 15 dias para que seja possível uma identificação mais precisa do baseline.
- Testes de configuração para validar o funcionamento correto da funcionalidade de desvio e de reinjeção de tráfego, garantindo que o processo de mitigação funcione corretamente, quando necessário. Para que o teste inicial aconteça de forma segura e transparente, é necessário que o CLIENTE informe um IP válido, sem uso. Caso não haja retorno por parte do **CLIENTE** para realização dos testes após três tentativas, o serviço será considerado ativo comercialmente.

- Para que seja possível a ativação de uma mitigação e com o objetivo de minimizar os riscos, o **CLIENTE** deverá fornecer à **Telefônica|Vivo** uma lista de contatos autorizados a decidir o início de uma mitigação. Esta lista não poderá exceder em 03 (três) pessoas e terá uma ordem de prioridade. A lista poderá ser modificada mediante uma solicitação ao nosso Centro de Relacionamento. As pessoas nas listas de autorizados poderão ser contatadas pela **Telefônica|Vivo** durante o horário 24x7x365. Ante uma detecção pró-ativa de um ataque, a **Telefônica|Vivo** realizará o contato, na ordem prevista, a qualquer pessoa desta lista.

2.5. Condições Gerais

2.5.1. Condições de Prestação do Serviço

2.5.1.1. Abertura de Chamados

As solicitações sobre o serviço, como dúvidas sobre a prestação dos serviços, faturamento, alteração de parâmetros, entre outros, deverão ser efetuadas a Central de Relacionamento da Vivo Empresas pelo telefone 0800 151551 código 9016. O atendimento é realizado 24 horas por dia, 7 dias por semana, 365 dias por ano.

O **CLIENTE** também possui um canal diretamente com o SOC no qual poderá reportar ataques e solicitar a mitigação reativa, com atendimento 24x7x365. Esta solicitação poderá ser feita através do número +55 (11) 969 010 762.

O **CLIENTE** poderá designar até 03 (três) administradores de sua empresa, unidade de negócio ou filial para contato com a Central de Relacionamento, os nomes deverão ser informados durante o processo de implantação do serviço. A Central de Relacionamento da Vivo Empresas não efetua atendimento ao usuário final.

O SOC efetuará o acompanhamento das solicitações e das soluções dadas ao **CLIENTE**. A cada solicitação será associado um número de registro da chamada e quando for o caso, um nível de severidade, conforme o grau crítico do problema avaliado.

2.5.1.2. Fechamento de Chamado

O chamado somente será concluído, pela Central de Relacionamento, com o "de acordo" dado por um dos três administradores designados previamente pelo **CLIENTE**, sendo o contato efetuado por telefone ou e-mail.

2.5.1.3. Horário de Atendimento

A prestação do serviço para atendimento aos ataques ocorre 24x7. O atendimento a consultas e modificações dos parâmetros de monitoração ocorre na modalidade 8x5.

2.5.1.4. Fluxo de Atendimento

Para controle das solicitações e da resolução das mesmas, bem como para o adequado acompanhamento do desempenho do serviço, o **CLIENTE** deve instruir e garantir que não haverá interação direta de seus usuários finais com a Central de Relacionamento da Vivo Empresas, sendo tal atividade atribuída apenas à equipe de suporte do **CLIENTE**.

No caso de necessidade de interação com o **CLIENTE** para a resolução de algum problema na infraestrutura de segurança do **CLIENTE**, a equipe técnica do SOC, através do Centro Técnico, entrará em contato com um dos três administradores designados pelo **CLIENTE**, que serão os pontos focais.

O ponto de contato do **CLIENTE** sempre será a Central de Relacionamento (nível 0), seja para abrir novas solicitações, reportar incidentes ou consultar o status de chamados abertos. A Central de Relacionamento é responsável por registrar todos os chamados dos Clientes. Uma vez que registrado, o chamado é direcionado para a Equipe de Supervisão do SOC (nível 1) que realiza a triagem e o primeiro atendimento, visando a resolução do chamado. Se necessário este chamado é direcionado a Equipe de Operação do SOC (nível 2) que é responsável por solucionar o chamado e, quando necessário, envolver parceiros tecnológicos (nível 3) para atender ao chamado do **CLIENTE**.

2.5.2. Suporte

O serviço contempla suporte com disponibilidade 24x7, para atender as consultas e solicitações do **CLIENTE**. Após a contratação do serviço, o **CLIENTE** receberá o procedimento de ação para casos de eventos e os telefones e correios eletrônicos destinados a qualquer solicitação e eventos no serviço.

2.5.2.1. Acordos do Nível de Serviço

Este item tem como objetivo estabelecer e fornecer informações a respeito do acordo de nível de serviço que irá definir os padrões de qualidade do serviço Anti-DDoS oferecido pela Vivo Empresas.

Este documento deve ser parte integrante e essencial do contrato de Prestação de Serviços firmado entre as partes e determinará os parâmetros necessários para orientar o andamento dos serviços. Também define as métricas para avaliação dos recursos e serviços disponibilizados, viabilizando a comparação dos resultados obtidos com as métricas estabelecidas, tanto em qualidade como quantidade e tempos de resposta do serviço. Além disso, constam desse documento os procedimentos necessários para o cumprimento do contrato.

2.5.2.1.1. SLO de prestação de serviços

O serviço de Anti-DDoS é prestado considerando os seguintes objetivos de atendimento.

2.5.2.1.2. SLO de Apresentação dos Relatórios

Serão medidos os seguintes prazos:

- ✓ Prazo de entrega de relatórios semestrais para a modalidade Básica e mensal para as demais modalidades: a partir do quinto dia do mês até o décimo.
- ✓ Prazo de entrega de relatórios de ataques: a partir da finalização do ataque até a entrega do relatório do ataque.

Indicador	Prazo
Tempo de entrega de relatórios de tráfego periódicos (semestrais ou mensais), conforme a modalidade.	Até 10º dia útil do mês subsequente ao período acordado
Tempo de entrega de relatório de incidente após a finalização de uma mitigação	5 dias úteis

SLO de Apresentação de relatórios

2.5.2.1.3. SLO de Solicitações e Consultas

Considera-se que as Solicitações e Consultas utilizarão os mesmos valores de SLOs que os de severidade baixa.

Indicadores de Consultas

Serão sujeitos a acordos de serviço os seguintes tempos:

- ✓ Tempo de atendimento a consultas: a partir da comunicação do **CLIENTE** até a atribuição do ticket a um analista do SOC
- ✓ Tempo de resolução de consultas: a partir da comunicação do **CLIENTE** até que o SOC comunique a resolução do mesmo

São previstas as seguintes consultas para este serviço:

- Lista de redes monitoradas;
- Alertas e mitigações;
- Informações sobre ataques recebidos
- Lista de contatos autorizados pelo **CLIENTE**.

Indicadores de Solicitações

Serão sujeitos a acordos de serviço os seguintes tempos:

- ✓ Tempo de atendimento a solicitações: a partir da comunicação do **CLIENTE** até a atribuição do ticket a um analista do SOC
- ✓ Tempo de resolução de solicitações: a partir da comunicação do **CLIENTE** até que o SOC comunique a resolução do mesmo

São previstas as seguintes solicitações para este serviço:

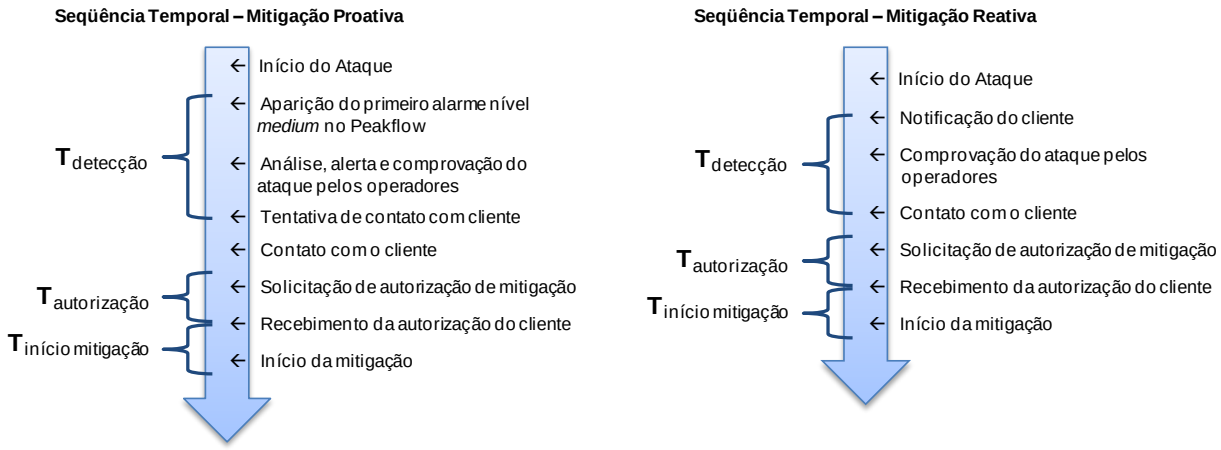
- Adicionar/retirar rede do monitoramento;
- Modificação na lista de contatos autorizados do **CLIENTE**;
- Modificação no mapa de serviços do **CLIENTE**;
- Solicitação de relatório de dados do tráfego do **CLIENTE** monitorado em um período específico.

Indicador	Crítico
Tempo de atendimento a partir da comunicação do CLIENTE até a atribuição do ticket a um analista do SOC	1h
Tempo de resolução a partir da comunicação do CLIENTE até que o SOC comunique a resolução do mesmo	10h
Tempo de atendimento de solicitações a partir da comunicação do CLIENTE até a atribuição do ticket a um analista do SOC	1h

Tabela 5 – SLO de **Solicitações e Consultas**

2.5.2.1.4. SLO de Mitigações de Incidentes

Para definir estes indicadores, utilizaremos os seguintes fluxos de atendimento, dependendo do tipo de detecção:



Mitigação - Sequencia Temporal

O tempo **T**autorização depende exclusivamente do **CLIENTE**, por consequência não é considerado como medida de qualidade do serviço. Serão, portanto, sujeitos a acordos de nível de serviços os seguintes tempos:

- **T detecção**
- **T início da mitigação**

Indicador	Crítico
Tempo de atendimento a partir da comunicação do CLIENTE até a atribuição do ticket a um analista do SOC.	15 min
Tempo de resposta a partir da aparição do primeiro alerta médium ate tentativa de contato com CLIENTE.	20 min
Tempo de início da mitigação a partir da autorização do CLIENTE até que a mitigação seja iniciada.	15 min
Tempo máximo de resposta para dúvidas relacionadas a um incidente aberto, alteração de parâmetros de mitigação em andamento, etc.	15 min.

SLO de **Mitigações de Incidentes**

2.5.2.1.5. SLO de Implantação

✓ A Vivo Empresas irá se reunir com a equipe técnica do **CLIENTE**, no prazo máximo de 15 (quinze) dias corridos após a assinatura do Contrato, para o planejamento da implantação do serviço a ser fornecido. Nesta reunião deverão ser discutidos e esclarecidos todos os questionamentos técnicos do serviço assim como as definições técnicas de configuração dos serviços e atividades de responsabilidade do **CLIENTE**.

✓ Prazo de implantação: 90 dias após a assinatura do Contrato, considerando o tempo desde que foram recebidas todas as informações do **CLIENTE** informações do **CLIENTE** (formulário de implantação) até o momento em que EGP – Escritório de Projetos - informa ao **CLIENTE** que todas as configurações foram realizadas e pode ser marcada uma data para o teste de implantação.

2.5.2.1.6. SLA de Prestação dos Serviços

Objetivo: garantir o atendimento de 95% dos SLOs por mês.

Somente se considera para efeitos de penalização:

- ✓ Incidentes Críticos e Altos;
- ✓ As requisições categorizadas como Altas pelo **CLIENTE** na abertura do chamado.

Assim, os itens que excedam não cumpram o SLA definido estarão sujeitos a um desconto, que serão liquidadas mensalmente pela fórmula:

$$Vpd = \frac{(Te \times 100)}{(1.440 \times Nd)}$$

Na qual:

- ✓ Vpd = percentual de minutos excedidos no respectivo mês;
- ✓ Te = tempo excedido em minutos além do determinado na tabela de SLO para o serviço em questão;
- ✓ Nd = Número de dias no mês

Sendo constatado o não cumprimento do SLA, os índices de descontos, da tabela, abaixo, serão aplicados sobre o valor mensal a ser pago pelo **CLIENTE**. Os descontos serão aplicados no mês subsequente ao mês da confirmação da ocorrência.

Percentual	Descontos %
0 < Vpd ≤ 2	0,5
2 < Vpd ≤ 4	1,0
4 < Vpd ≤ 6	2,5
6 < Vpd ≤ 10	5,0
10 < Vpd ≤ 20	7,5
Vpd > 20	10,0

Índices de descontos

2.5.2.1.7. Interrupções

A disponibilidade que garante o serviço obedece às seguintes condições:

- ✓ Não se contabilizarão dentro do tempo da não disponibilidade as interrupções do serviço que foram provocadas por causas imputáveis ao **CLIENTE**;
- ✓ O **CLIENTE** está obrigado a facilitar o acesso a suas dependências, das pessoas designadas pela Vivo Empresas, para a resolução dos problemas, ou a operação do serviço que seja necessária. O tempo necessário para obter esta permissão está fora do cálculo da disponibilidade;
- ✓ A Vivo Empresas se reserva no direito de efetuar, mediante aviso prévio ao **CLIENTE**, paradas técnicas que não se contabilizam no cômputo da disponibilidade;
- ✓ São excluídas interrupções do serviço devidas a causas de força maior (por exemplo, desastres naturais).

2.5.2.1.8. Períodos de manutenção

Por necessidade de manutenção, pode ser necessário interromper o serviço prestado ao **CLIENTE**, com o objetivo de executar reconfigurações, atividades de manutenção, etc., na plataforma

de prestação de serviços. Tais atividades serão executadas, necessariamente, durante um período pré-programado de manutenção.

2.5.2.1.9. Interrupções programadas

As interrupções programadas de disponibilidade do serviço sejam elas pelas causas motivadas pelo item anterior, de períodos de manutenção, ou motivadas por alguma solicitação do **CLIENTE**, não serão contabilizadas para o cálculo da disponibilidade do serviço,

2.6. Responsabilidades do CLIENTE

Clientes que venham a contratar serviços da Vivo Empresas estarão assumindo as seguintes responsabilidades:

- ✓ Informar a Vivo Empresas sobre qualquer mudança com relação à prestação dos serviços, com a devida antecedência, permitindo que a mesma tenha tempo suficiente para preparar e implementar as alterações necessárias, conforme tais alterações ou mudanças afetem a prestação dos serviços. O **CLIENTE** deverá fornecer informações suficientes com relação às suas necessidades;
- ✓ Informar a Vivo Empresas com antecedência mínima de 30 (trinta) dias sobre qualquer mudança que possa afetar a prestação de Serviços
- ✓ Zelar pela conservação e correto manuseio da infraestrutura disponibilizada pela Vivo Empresas, responsabilizando-se pelos eventuais danos, pessoais e materiais, decorrentes de ações e utilizações indevidas por parte de seu pessoal ou de seus equipamentos;
- ✓ Informar internamente e aos seus outros prestadores de serviços, o escopo de contrato com a Vivo Empresas, quando relacionado a suas atividades;
- ✓ Não gerenciar diretamente nenhum funcionário ou terceiros da Vivo Empresas alocados ou em atendimento nos sites do **CLIENTE**.
- ✓ Providenciar as autorizações de ingresso do pessoal da Vivo Empresas às suas instalações para executar o projeto contratado (caso for necessário).
- ✓ Designar um único interlocutor como responsável pelo projeto, e definir as pessoas de contato autorizadas a realizar consultas.
- ✓ Analisar o produto gerado e aprová-lo quando corresponder, garantindo a continuidade das diversas atividades do projeto e possibilitando seu fechamento quando os requisitos definidos para o projeto forem atendidos.
- ✓ Brindar a correspondente diligência nos trabalhos que lhe sejam próprios a executar dentro dos prazos do planejamento proposto.
- ✓ Designar o pessoal necessário, especializado nas funções a realizar e com dedicação suficiente a essas tarefas, para coordenar e entregar a Vivo Empresas a informação necessária para análise e resolução de eventos.
- ✓ Proporcionar, conforme corresponda, a infraestrutura necessária para instalação de equipes, cumprindo com as especificações indicadas nesta oferta.

2.7. Responsabilidades da Vivo Empresas

A Vivo Empresas assume as seguintes responsabilidades perante os Clientes que venham a contratar seus serviços.

- ✓ Designar um profissional da Vivo Empresas que será ponto focal para o projeto;
- ✓ Tornar disponíveis recursos Vivo Empresas necessários para execução dos serviços;
- ✓ Executar os serviços de acordo com os objetivos de níveis de serviço;
- ✓ Executar todas as atividades dentro dos padrões de qualidade Vivo Empresas e conforme estabelecido no contrato com o **CLIENTE**;
- ✓ Cumprir os prazos estabelecidos nas atividades do projeto, desde que as responsabilidades do **CLIENTE**, sejam cumpridas;
- ✓ Gerenciamento proativo do serviço incluindo o fornecimento da Central de Atendimento.
- ✓ Dirigir, organizar e gerenciar o projeto.
- ✓ Participar nas reuniões de trabalho combinadas.
- ✓ Manter informado o pessoal do **CLIENTE**, sobre ações e resultados nas diferentes atividades.
- ✓ Garantir a confidencialidade dos dados informados pelo **CLIENTE**, para o desenvolvimento da atividade.
- ✓ O pessoal da Vivo Empresas que tiver acesso aos escritórios do **CLIENTE**, estará sujeito às normas de segurança que o **CLIENTE**, estabelecer para acesso e permanência em suas instalações.
- ✓ Comunicará e solicitará ao **CLIENTE**, a aprovação explícita de qualquer mudança da equipe de trabalho, com uma antecipação mínima de sete (7) dias corridos.

2.8. Prazo de Implantação

A Vivo Empresas irá se reunir com a equipe técnica do **CLIENTE**, no prazo máximo de 15 (quinze) dias corridos após a instalação do acesso, para o planejamento da implantação do serviço a ser fornecido. Nesta reunião deverão ser discutidos e esclarecidos todos os questionamentos técnicos do serviço assim como as definições técnicas de configuração dos serviços e atividades de responsabilidade do **CLIENTE**.

O prazo máximo para disponibilização do serviço de Proteção DoS será de até 30 dias (trinta dias), após instalação do acesso, salvo negociação específica com as áreas operacionais a ser realizada durante a fase de elaboração da proposta. Este prazo não contempla a disponibilização de equipamentos, no caso de vendas ou locação, assim como os prazos de instalação de links de dados, quando inclusos nos projetos. Limitações ou situações específicas de cada **CLIENTE** e projeto podem causar variação nos prazos estabelecidos.

Ao finalizar o período de provisão do serviço, o **CLIENTE** e Vivo Empresas acordarão testes de configuração para verificar o funcionamento correto de funcionalidade de desvio de tráfego e reinserção de tráfego e garantir que o serviço funcione corretamente. Com o objetivo de customizar os limiares de detecção para aperfeiçoar o serviço ao **CLIENTE**, a Vivo Empresas solicitará ao **CLIENTE**, informações específicas de sua infraestrutura de rede interna e equipamento de segurança existente. Tais informações serão confidenciais e não poderão ser divulgadas pela Vivo Empresas.