UNIVERSIDADE DO EXTREMO SUL CATARINENSE – UNESC

CURSO DE CIÊNCIA DA COMPUTAÇÃO

HARILTON RICARDO DE SOUSA DIAS

AVALIAÇÃO DE UMA CONTRAMEDIDA DE MITIGAÇÃO CONTRA ATAQUES DE NEGAÇÃO DE SERVIÇO BASEADA NA *CLOUD COMPUTING*

CRICIÚMA

2016

HARILTON RICARDO DE SOUSA DIAS

AVALIAÇÃO DE UMA CONTRAMEDIDA DE MITIGAÇÃO CONTRA ATAQUES DE NEGAÇÃO DE SERVIÇO BASEADA NA *CLOUD COMPUTING*

Trabalho de Conclusão de Curso, apresentado para obtenção do grau de Bacharel no curso de Ciência da Computação da Universidade do Extremo Sul Catarinense, UNESC.

Orientador: Prof. Msc. Paulo João Martins

CRICIÚMA

2016

HARILTON RICARDO DE SOUSA DIAS

AVALIAÇÃO DE UMA CONTRAMEDIDA DE MITIGAÇÃO CONTRA ATAQUES DE NEGAÇÃO DE SERVIÇO BASEADA NA *CLOUD COMPUTING*

Trabalho de Conclusão de Curso aprovado pela Banca Examinadora para obtenção do Grau de Bacharel, no Curso de Ciência da Computação da Universidade do Extremo Sul Catarinense, UNESC, com Linha de Pesquisa em Segurança de Sistemas Computacionais.

Criciúma, 01 de dezembro de 2016.

BANCA EXAMINADORA

Prof. MSc. Paulo João Martins - (UNESC) - Orientador

Prof. MSc. Rogério Antônio Casagrande - (UNESC) - Membro Banca

Prof. Esp. Valter Blauth Junior - (UNESC) - Membro Banca

A Deus pelas bênçãos, à minha mãe, Celeste, por estar sempre do meu lado, sempre me motivando e amparando nos bons e maus momentos.

AGRADECIMENTOS

Primeiramente agradeço a Deus, pela sua presença, proteção e sabedoria, aos meus pais Ângelo Armando Almeida Dias e Celeste Caldeira de Sousa, por todo apoio moral e sentimental. Agradeço especialmente a minha mãe por ser uma supermulher, pelo seu amor e esforço incalculável ao abrir mão de certas coisas para me ver bem e terminar os meus estudos.

Ao meu tio José Manuel Caldeira de Sousa Barros por me direcionar a este ramo de atuação, a minha querida tia Maria Filomena Caldeira de Sousa por todas orações e ensinamentos, e a minha querida tia Sandra Marlene Dias da Silva por todo carinho e apoio.

Aos meus irmãos Ercília, Jacira, Jorson, Albino e Mandinho Dias, pelo carinho e por torcerem por mim.

Agradecimentos especiais à Gisele Dagostin, pelo apoio, pela motivação, pela confiança, pela paciência e por toda ajuda para a idealização desta pesquisa, o meu muito obrigado.

Aos meus amigos que contribuíram de forma direta ou indireta, obrigado pelo incentivo e apoio Célio Filipe, e pelas palavras de conforto Sílvia Victoriano, Moustapha Seck, Pedro Figueira, Anaclécio Dala, Brawlio Fonseca, Carlos Barros...

Ao meu amigo e coordenador do Polo UAB de Criciúma Júlio César Viana, pela compreensão, pela confiança e por disponibilizar os recursos necessários para a execução dos testes desta pesquisa.

À Maxihost, particularmente ao Sr. Guilherme Soubihe e o engenheiro de segurança Roni Lima, pela oportunidade concedida, pela confiança, pela parceria e por todo apoio para o desenvolvimento desta pesquisa.

À Universidade do Extremo Sul Catarinense (UNESC) e seu quadro docente, pelo suporte e por todo apoio durante esta jornada, e ao meu orientador Paulo João Martins, pelas ideias e apoio.

Finalizo agradecendo a todos que direta ou indiretamente contribuíram para me tornar o homem que hoje sou.

O meu muito obrigado!

“Se você fez alguma coisa e ela se revelou muito boa, então você deveria ir fazer outra coisa sensacional e não se preocupar com isso por muito tempo. Apenas entenda o que vem a seguir.”

Steve Jobs

RESUMO

Em um mercado cada vez mais competitivo e cercado de vulnerabilidades e ameaças digitais, é necessário que as organizações adotem proporcionalmente soluções adequadas de monitoramento e proteção para os seus ativos. Ataques de Negação de Serviço (*Denial of Service* - DoS) representam uma destas ameaças. Este tipo de ameaça afeta diretamente a qualidade de serviço (*Quality of Service - QoS*) e a quantidade de recursos disponíveis em uma rede, impedindo que seus usuários legítimos tenham acesso e realizam suas atividades. O estudo desta pesquisa, consistiu na avaliação de uma contramedida de mitigação contra-ataques DoS baseada na cloud computing e nos seus modelos de serviço. Para a sua concepção, seguiu-se a seguinte metodologia: pesquisa bibliográfica, e a elaboração de um estudo de caso onde aplicou-se quatro (4) etapas, nomeadamente: autorização das entidades envolvidas, preparação do cenário de aplicação, leitura e extração dos dados, e documentação dos resultados obtidos. Os dados foram obtidos a partir de dois painéis de monitoramento fornecidos pela empresa envolvida no estudo. Os resultados auxiliam os profissionais de segurança a entender e a lidar com os riscos de ataques DoS, além de reduzirem a carga sob analistas e administradores de redes. Com isto posto, subentende-se que a presente pesquisa alcançou com sucesso o seu propósito.

Palavras-chave: Negação de Serviço. Tráfego de Rede. Segurança da Informação.

ABSTRACT

In an increasingly competitive market and surrounded vulnerabilities and digital threats, it is necessary that organizations adopt proportionally appropriate solutions for monitoring and protection for its actives. Denial of Service (DoS) attacks represent one of these threats. This type of threat directly affects the Quality of Service (QoS) and the amount of available resources on a network, preventing their legitimate users from accessing and performing their activities. The study of this research, consisted of the evaluation of a mitigation countermeasure based on cloud computing and its service models. For its conception, the following methodology was used: bibliographic research, and the elaboration of a case study where four (4) steps were applied, namely: authorization of the entities involved, preparation of the application scenario, reading and extraction of data, and documentation of results obtained. Data were obtained from two monitoring panels provided by the company involved in the study. The results help security professionals understand and deal with the risks of DoS attacks, yon reduce the burden on analysts and network administrators. With this post, it is understood that the present research successfully achieved its purpose.

Keywords: *Denial of Service. Network Traffic. Information Security.*

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ACL	Lista de Controle de Acesso
ADS	*Anti-DoS System*
ADSL	*Asymmetric Digital Subscriber Line*
ADSM	*Anti-DoS System Manager*
API	*Application Programming Interface*
avg	*Average*
AWS	*Amazon Web Service*
bps	*Number of Bits*
CERT.br	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CERT.org	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança nos Estados Unidos da América
CIO	*Chief Information Officer*
CMS	*Content Management System*
CNN	*Cable News Network*
CPE	*Customer Premises Equipment*
CPU	*Central Processing Unit*
DaaS	Banco de Dados como Serviço
DDoS	*Distributed Denial of Service*
DNS	*Domain Name System*
DoS	*Denial of Service*
DRDoS	*Distributed Reflection Denial of Service*
FTP	*File Transfer Protocol*
Gbps	*Gigabits* por Segundo
GHz	*Gigahertz*
GRE	*Generic Routing Encapsulation*
HP	*Hewlett Packard*
IaaS	Infraestrutura como Serviço
ICMP	*Internet Control Message Protocol*
IDPS	*Intrusion Detection and Prevention Systems*
IDS	*Intrusion Detection System*

IP	*Internet Protocol*
IPS	*Intrusion Preventy System*
IPSec	*Internet Protocol Security*
IPv4	*Internet Protocol 4th Version*
IPv6	*Internet Protocol 6th Version*
IRC	*Internet Relay Chat*
ISP	*Internet Service Provider*
max	*Maximum*
Mbps	*Megabits per second*
min	*Minimum*
NFA	*Network File System*
NIC.br	Núcleo de Informação e Coordenação no Brasil
NIST	*National Institute of Standards and Technology*
NTA	*Network Traffic Analyzer*
NTP	*Network Time Protocol*
OMC	Organização Mundial do Comércio
OSI	*Open Systems Interconnect*
PaaS	Plataforma como Serviço
PFN	*Protection for Networks*
PING	*Packet Internet Network Grouper*
pps	*Packets per Second*
ppu	*Pay per Use*
PSI	Políticas de Segurança da Informação
QoS	*Quality of Service*
RAM	*Random Access Memory*
RDP	*Remote Desktop Protocol*
RFC	*Request for Comments*
Rsh	*Remote shell*
SaaS	Software como Serviço
SI	Sistema de Informação
SIG	Sistema de Informação Gerencial
SLA	*Service Level Agreement*
SMTP	*Simple Mail Transfer Protocol*
SNMP	*Simple Network Management Protocol*

SSDP	*Simple Service Discovery Protocol*
SSH	*Secure Shell*
SSL	*Secure Sockets Layer*
TCP	*Transmission Control Protocol*
TI	Tecnologia da Informação
TTL	*Time to Live*
UAB	Universidade Aberta do Brasil
UDP	*User Datagram Protocol*
UNESC	Universidade do Extremo Sul Catarinense
UPnP	*Universal Plug and Play*
URL	*Uniform Resource Locator*
UTC	*Coordinated Universal Time*
VoIP	*Voice over IP*
VPN	*Virtual Private Network*
WEB	*World Wide Web*

SUMÁRIO

1 INTRODUÇÃO

Existe um consenso na nossa sociedade de que o bem mais valioso do século XXI é a informação. Os últimos anos foram marcados pela propagação progressiva de equipamentos de comunicação, deixado de ser o computador o único meio tecnológico e digital do nosso dia a dia, percorrendo por outros tipos de dispositivos, particularmente os dispositivos móveis como *smartphones*, *tablets*, *smartwatches*, assistentes virtuais, entre outros. Consequentemente, existe uma grande disseminação de informações estratégicas e de grande importância que circulam na maior infraestrutura de rede pública de comunicação, à Internet (CARISSIMI; ROCHOL; GRANVILLE, 2009).

Com todas estas informações a circular em uma infraestrutura de rede pública, estende-se há necessidade de garantir a proteção destes ativos frente as inúmeras ameaças a que estão sujeitos. *Worms*, vírus, engenharia social, *malwares*, *keyloggers*, entre outras ameaças, representam o cenário a que estamos expostos. Contudo, esta pesquisa centraliza o seu estudo nos ataques de Negação de Serviço (*Denial of Service* - DoS) e na sua variável distribuída, os ataques Distribuídos de Negação de Serviço (*Distributed Denial of Service* - DDoS). Os seus intentos, visam esgotar todos os recursos disponíveis em um servidor através da produção de tráfego malicioso, que resulta na queda parcial ou total de um servidor.

A implementação de um modelo avançado e de estratégias de gestão, proteção e monitoramento de tráfego de rede em tempo real, garantem uma maior produtividade, um maior desempenho e qualidade na entrega de serviços e ferramentas aos usuários legítimos da rede.

No decorrer dos anos, vários serviços e ferramentas para combater ataques de negação de serviço foram desenvolvidas. Esta pesquisa visa explorar uma solução inovadora de proteção baseada na *cloud computing*, que propõe o estudo de um caso onde é realizado um ataque DoS controlado, e a aplicação de uma contramedida de mitigação baseada na *cloud computing*.

1.1 OBJETIVO GERAL

Monitorar o tráfego de dados em um ambiente *cloud* público de uma rede e descrever uma contramedida de mitigação contra-ataques de negação de serviço baseada na *cloud*.

1.2 OBJETIVOS ESPECÍFICOS

Em conformidade ao objetivo geral, os objetivos específicos desta pesquisa foram:

a) descrever sobre a importância dos sistemas de informação e sua segurança;
b) compreender os protocolos utilizados para a concepção de ataques DoS;
c) pesquisar e utilizar ferramentas que interceptam e analisam o tráfego de uma rede;
d) entender sobre os conceitos negação de serviço, *cloud computing*, rede de distribuição de conteúdo, mecanismos e serviços IDS/IPS, entre outros;
e) descrever o ambiente utilizado e definir os cenários;
f) recolher e analisar os dados obtidos no ambiente de teste, bem como documentar os resultados obtidos.

1.3 JUSTIFICATIVA

Em um mundo globalizado e cada vez mais interconectado, garantir a segurança em redes de computadores tornou-se um problema da atualidade, a Internet se transformou num oceano de transações de informações, sendo elas muito importantes para as organizações bem como para benefícios pessoais (CAPITANGO, 2011).

Fato é, que o homem passou a manipular, obter, descartar, e gerir informações em centenas de milhares de dispositivos, sejam estes fixos ou móveis.

Todo este número de ligações e troca de informações gera um enorme tráfego em redes de computadores (SILVA, 2015).

Um ataque de negação de serviço ocorre quando um servidor ou site recebe uma sobrecarga de tráfego, ou seja, muito mais tráfego ou pedidos que ele possa atender, fazendo com que falhe (TURBAN; VOLONINO, 2013).

Estes ataques têm surgido com maior frequência, maior volume de tráfego e cada vez mais tornam-se difíceis de serem bloqueados e mitigados, espera-se então sistemas e contramedidas que sejam capazes de proteger sem afetarem o correto funcionamento de infraestruturas de TI (PEREIRA, 2014).

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (Cert.br), apontou que recebeu 223.935 notificações de incidentes por conta dos ataques DoS, um aumento de 197%, ou seja, um número 217 vezes maior que o registrado em 2013. Esses tipos de ataques não apenas comprometem o ativo mais valioso das instituições, mas também geram um volume de tráfego muito alto (NIC.br, 2015).

Já o estudo conduzido pela *Nexusguard*, empresa líder global em soluções de segurança, apontou no seu primeiro trimestre de estudo que o Brasil é o terceiro maior alvo de ataques DoS/DDoS do mundo, e o primeiro da *América Latina*. Ao todo, foram avaliados 180 países, *Estados Unidos* e *China* ocuparam as primeiras posições (Nexusguard, 2016, traduçã nossa).

Desta forma, recomenda-se que as organizações adotem soluções e estratégias de monitoramento e proteção, de modo a não comprometerem as suas operações de TI (MAXIHOST, 2016a).

O tipo de abordagem adotada por muitas organizações reflete na propagação de crimes digitais, já que adotam abordagens reativas e que só após detecção do problema, permitem tomar contramedidas.

Nesta pesquisa propõe-se, avaliar uma contramedidade proativa de bloqueio e mitigação no combate aos ataques DoS/DDoS.

1.4 TÓPICOS DO TRABALHO

Esta pesquisa está pautada em seis capítulos. O primeiro contém a Introdução, e a descrição geral da pesquisa, descrevendo o problema, a justificativa, o objetivo geral, e os objetivos específicos.

O segundo capítulo, Sistemas de Informação, aborda o rápido crescimento e evolução que os sistemas de informação sofreram na atualidade, assim como, a necessidade de proteger a informação nas organizações. Outros aspetos associados ao tema são apresentados.

O terceiro capítulo, Segurança em Redes de Computadores, define seus principais conceitos, técnicas de proteção, estatísticas do Cert, causas, tipos, e diferença dos ataques DoS, além do papel que as políticas de segurança exercem nas organizações.

O quarto capítulo, *Cloud Computing*, consiste especialmente nas vantagens e benefícios que a tecnologia oferece essencialmente como serviço, e no estudo da contramedida utilizada para mitigação.

O quinto capítulo, Trabalhos Correlatos, relaciona alguns dos trabalhos da comunidade acadêmica e científica ligados a esta pesquisa.

O sexto capítulo, Trabalho Desenvolvido, retrata a abordagem metodológica adotada, e o estudo de caso feito, onde foi executado um ataque DoS controlado, seguindo da demonstração de uma contramedida de mitigação baseada na *cloud computing* para a respetiva ameaça.

O sétimo capítulo, Conclusão, descreve resumidamente todo trabalho feito, partindo dos resultados obtidos as dificultades encontradas no decorrer do seu desenvolvimento. Ao final, algumas outras linhas de pesquisa são descritas para o desenvolvimento de trabalhos futuros.

2 SISTEMAS DE INFORMAÇÃO

Há muito, as empresas têm sido influenciadas por transformações e inovações que surgem no mercado, onde nos últimos anos registram e vivenciam a velocidade da evolução na era da informação[1]. No mundo moderno as organizações não só devem se preocupar com a competição global, mas também em como manter protegido o seu ativo mais valioso, a informação (SÊMOLA, 2014).

Um Sistema de Informação (SI) é um conjunto de componentes inter-relacionados, utilizados para sentir, comunicar, analisar e apresentar informações com o propósito de melhorar nossa capacidade de perceber, compreender controlar e criar (LAUDON; LAUDON, 2014).

Sistemas de Informação são conhecidos mundialmente, e exercem impacto em diferentes áreas como, na exploração de formas inovadoras de aplicação de tecnologia, visto que têm despertado um crescente interesse a nível mundial, em razão ao seu constante e rápido progresso (RAY; ACHARYA, 2004, tradução nossa). Diante deste cenário, as organizações passaram a lidar com um aumento de ameaças, no entanto, a sua capacidade de revolucionar estas ameaças permite criar novas oportunidades de negócio e oferecer a possibilidade de reduzir custos (CASCARINO, 2012, tradução nossa). Todavia, é necessário que as empresas se adaptem rapidamente às novas condições, no sentido de progredir, competir e até sobreviver (CARNEIRO, 2009).

Para perceber como os sistemas de informação são importantes, pode-se analisar o estudo conduzido por Laudon e Laudon (2014), onde retrata a notável e enorme valorização que o mundo do esporte obteve nas últimas décadas, que embora esporte, é uma das atividades humanas mais praticadas e vistas. Trata-se do estádio do *New York Yankees.* No estudo, os autores descrevem os desafios que os engenheiros tiveram para criar o estádio mais cabeado, conectado e com disposição para vídeo, oferecendo mais espaço e conforto. Para que tudo isso fosse possível, a solução foi à aplicação de sistemas de informação.

[1] Dados que passam por algum tipo de processamento para que possam ser utilizados de maneira inteligível (DANTAS, 2011).

2.1 A INFORMAÇÃO NA ERA DIGITAL

A principal diferença que irá surgir na informação do futuro, é que toda ela será no formato digital. Bibliotecas inteiras já estão sendo armazenadas em discos ou *CD-ROMs*, sob o formato de dados eletrônicos. Jornais e revistas hoje em dia, são na maioria das vezes compostos inteiramente em formato digital e impressos em papel por conveniência de distribuição. A informação eletrônica digital é armazenada permanentemente, ou por quanto tempo se deseje, em bancos de dados computadorizados, e em gigantescos bancos de dados jornalísticos, acessíveis por meio de serviços on-line (GATES, 1995).

O mundo moderno tem dedicado especial atenção a informação, devido a sua importância para a preservação dos negócios e a realização de novos empreendimentos entre pessoas, empresas, povos, nações e blocos econômicos (DANTAS, 2011).

Ainda em conformidade a uma previsão feita por Gates (1995), pequenos dispositivos seriam criados e caberiam em nossos bolsos, permitiriam manter contato com pessoas, ver informações sobre voos, sobre negócios, detalhes do mercado financeiro a tempo integral, ou seja, surgiria então a era do *smartphone*. Estes dispositivos tornar-se-iam também nossos assistentes pessoais, sendo capazes de conectar e sincronizar todos os seus dispositivos de uma forma inteligente, verificar nossos e-mails, entre outras ações, tanto no escritório quanto em casa.

Os tempos se passaram, várias mudanças surgiram e hoje, as previsões feitas por Gates acabaram por se realizar. Vivenciamos a evolução contínua destes pequenos dispositivos, os smartphones. Estes dispositivos encontram-se em evidêndia pela sua alta capacidade de processamento, que se comparados, chegam a apresentar superioridade em relação a alguns modelos de computadors pessoais. Destaca-se também, a total integração que estes dispositivos passaram a ter com os serviços de Internet e com os ambientes em nuvem.

2.2 SEGURANÇA DA INFORMAÇÃO

No contexto da norma, a segurança da informação é a proteção contra vários tipos de ameaças para assegurar a continuidade do negócio, reduzir o risco,

potencializar o retorno sobre os investimentos e as oportunidades do negócio, ou seja, preservar a confidencialidade, integridade, e disponibilidade da informação; ampliando as demais propriedades, autenticidade, responsabilidade, não repúdio e confiabilidade (NBR ISO/IEC 27002, 2013).

Em rede de computadores existem diversas técnicas e ferramentas físicas ou lógicas que consistem na proteção, controle de acesso e consequentemente no combate de ataques. Todos estes mecanismos têm um papel importante na gestão da informação. Algumas destas técnicas e ferramentas foram abordadas (SÊMOLA, 2014):

a) ***firewalls*:** é um sistema de segurança físico ou lógico, baseado no controle da entrada e saída do tráfego de uma rede por meio de regras (ROUSE, 2014, tradução nossa);
b) **criptografia:** Stallings (2008) explica que uma mensagem original é conhecida como texto claro, ou *plaintext*, enquanto a mensagem codificada é chamada de texto cifrado, ou *ciphertext.* O processo que consiste em converter esse texto claro em texto cifrado é conhecido como cifragem ou criptografia;
c) **sistemas de detecção de intrusos:** do inglês *Intrusion Detection Systems* (IDS), é um dispositivo adicional ao firewall que permite analisar os cabeçalhos de todos os pacotes e executar uma inspeção mais profunda nestes pacotes (KUROSE; ROSS, 2010);
d) **sistemas de prevenção de intrusos:** do inglês *Intrusion Prevention Systems* (IPS), é a evolução do IDS e tem de novo, a capacidade de não só alertar, mas também tomar ações predeterminadas, seja o bloqueio de pacotes de dados ou ataques que representem uma situação de risco. *Intrusion Detection and Prevention Systems* (IDPS) é a junção destes dois sistemas (SÊMOLA, 2014).

Outros mecanismos podem também ser utilizados no combate de ataques e invasões, é o caso dos antivírus[2], *anti-spam*[3], *anti-spyware*[4], *anti-phishing*[5] entre outros. Não há dúvidas que estas ferramentas e tecnologias são necessárias e devem

[2] Ferramenta que procura detetar e, anular ou remover códigos maliciosos (CERT.br, 2012a).
[3] Programa que permite separar os e-mails conforme as regras pré-estabelecidas (CERT.br, 2012a).
[4] Ferramenta para impedir que programas com código malicioso monitorem as atividades de um sistema (CERT.br, 2012a).
[5] Programa ou filtro para impedir o roubo de dados pessoais e financeiros (CERT.br, 2012a).

ser implementadas, entretanto, podem não ser suficientes visto que essas ferramentas e tecnologias podem possuir certas limitações dependendo dos investimentos feitos.

Nota-se uma similaridade nos conceitos que a literatura vem apresentando referente a segurança da informação, que é a preservação dos seus elementos: confidencialidade, integridade e disponibilidade, conhecidos por diversos autores como CID. Estes três elementos são os três pilares principais da segurança da informação (LYRA, 2015).

Seguindo os padrões internacionais, a segurança da informação precisa sempre atender os seus três elementos básicos (RAMOS, 2008):

a) **confidencialidade:** uma informação só pode ser acessada por quem possui um determinado nível de privilégio ou autorização, ou seja, basicamente, estamos falando de sigilo;
b) **integridade:** implica no facto que uma informação só pode ser modificada por quem tem a devida autorização para o fazê-lo. Estas modificações podem ser tanto intencionais quanto acidentais;
c) **disponibilidade:** uma informação deve estar sempre disponível para quem for autorizado e necessitar consultá-la. Esta informação ou o meio informático (sistema, servidores, entre outros) deve estar disponível 24h por dia, 7 dias por semana. A figura 1 complementa a explicação.

Figura 1 - Segurança da Informação: Tríade CIA.

Fonte: NBR ISO/IEC 27001 (2013).

Todavia, outras correntes defendem a adoção de outros atributos complementares para garantir a segurança da informação (LYRA, 2015):

a) **autenticidade:** cada parte envolvida deve ser quem ela diz ser, ou seja, é necessário garantir a identificação das mesmas (LYRA, 2008);
b) **auditoria:** consiste na coleta de evidências de uso dos recursos existentes, a fim de identificar cada parte envolvida em um processo de troca de informações, ou seja, origem, destino e meios de tráfego de uma informação (CARISSIMI; ROCHOL; GRANVILLE, 2009);
c) **legalidade:** garante que o sistema esteja de acordo com a legislação (LYRA, 2015);
d) **não-repúdio:** um mecanismo de veracidade permite identificar a origem de um determinado documento, não sendo possível o remetente negar que gerou, ou enviou uma determinada mensagem ou documento (CARISSIMI; ROCHOL; GRANVILLE, 2009);
e) **privacidade:** um sistema deve ser capaz de preservar a identidade de um usuário, não permitindo o relacionamento entre o usuário e suas ações (LYRA, 2008).

2.3 ASPETOS DA SEGURANÇA DA INFORMAÇÃO

Alguns conceitos básicos são considerados fundamentais na prática da segurança da informação independentemente do objetivo que se pretende alcançar. Anteriormente foi abordado sobre os três pilares principais da segurança da informação (confidencialidade, integridade e autenticidade), todavia, é importante também estudar sobre outros conceitos que são pertinentes à segurança de uma rede de computadores.

2.3.1 Ativo de informação

Para que a segurança da informação seja alcançada, é necessário antes de mais cumprir com alguns pontos, seja um conjunto de práticas e atividades como a definição ou elaboração de processos, políticas de segurança da informação, procedimentos, treinamento de profissionais, uso de ferramentas de monitoramento e controle, entre outros. Portanto, é crucial proteger aquilo que tenha valor para as

organizações: os ativos de informação como as informações (dados, projetos, entre outros), pessoas e suas qualificações, serviços de tecnologia, ativos físicos (equipamentos de *hardware*), ativos de *software* (aplicativos, sistemas, entre outros), reputação da empresa e outros serviços físicos (iluminação, eletricidade, entre outros) (LYRA, 2015).

2.3.2 Ameaça

São agentes ou condições responsáveis por causar danos aos negócios de uma organização, danos estes que comprometem as informações e seus ativos mediante da exploração de vulnerabilidades, resultando em perdas de confidencialidade e disponibilidade. As ameaças quanto a sua intencionalidade podem ser classificadas em naturais, involuntárias e voluntárias (SÊMOLA, 2014).

2.3.3 Mitigação

São todas ações adotadas que permitem diminuir o risco em relação a uma subjacente ameaça (MICROSOFT, 2006, tradução nossa).

2.3.4 Vulnerabilidade

Refere-se a uma condição que, no momento em que explorada por um atacante, pode suceder em uma violação de segurança. São exemplos de vulnerabilidades, falhas em projetos, má implementação ou configuração de programas, serviços ou equipamentos de rede (CERT.br, 2012a).

2.3.5 Negócio

Laudon e Laudon (2014) explicam que o uso da Internet e da tecnologia digital para a execução de todos os processos da empresa, incluindo o comércio eletrônico, tal como os processos de gestão interna e coordenação dos fornecedores e outros parceiros, definem o conceito de negócio. Sistemas de informação permitem automatizar muitas das etapas que antes eram executadas manualmente. Por

exemplo, verificar o crédito de um cliente, gerar uma ordem de fatura, a criação de novos modelos de negócio, entre outras vantagens.

2.3.6 Risco

O Guia de Gerenciamento de Riscos da Microsoft (2006, tradução nossa), determina que o risco está associado a probabilidade de um evento e a sua consequência.

Sêmola (2014), complementa ao explicar que o risco é a probabilidade de que agentes (ameaças), venham a explorar vulnerabilidades, tendo como consequência, a exposição dos ativos resultando em perdas de confidencialidade, integridade e disponibilidade, e causando impactos nos negócios. Para lidar com esses impactos e proteger seus ativos, as organizações implementam medidas de segurança, impossibilitando que ameaças explorem as vulnerabilidades, diminuindo assim, o risco. A equação do risco (1) é representada pelas variáveis, vulnerabilidades, ameaças, impactos e medidas de segurança:

$$R = \frac{V \;\; x \;\; A \;\; x \;\; I}{M} \qquad (1)$$

Onde: R é o risco; V são as vulnerabilidades, A ameaças, I o impacto e M as medidas de segurança.

3 SEGURANÇA EM REDES DE COMPUTADORES

A Internet oferece aos seus usuários uma enorme diversidade de serviços, como navegação WEB, mensagens de texto, *streaming* de música e vídeo, comunicação VoIP, entre ouros serviços. Todavia, há uma necessidade em manter a qualidade e segurança desse sistema global de redes (COMER, 2016).

Para um melhor entendimento, será feita uma analogia clássica de dois namorados, Alice e Bob, e de Trudy, à intrusa. Eles pretendem se comunicar com segurança. Alice quer enviar uma mensagem a Bob, e quer que somente ele receba a mensagem, mesmo que ela seja transmitida de um meio inseguro, onde Trudy pode interceptar qualquer dado que seja transmitido entre o casal. De igual modo, Bob também quer ter certeza que a mensagem recebida é de Alice e foi enviada por ela, assim como Alice quer ter certeza que de fato está a se comunicar com Bob. Eles ainda precisam ter certeza que as suas mensagens não foram alteradas em trânsito. E principalmente, querem antes de tudo, ter certeza que podem se comunicar, isto é, que ninguém lhes negue acesso aos recursos necessários para a comunicação (KUROSE, 2010).

Para garantir a segurança em uma rede de computadores não é diferente, é necessário garantir que apenas o remetente e o destinatário possam entender o conteúdo da mensagem enviada (confidencialidade), que seja confirmada a identidade da outra parte envolvida na comunicação (autenticação), que o conteúdo de sua comunicação não seja alterado (integridade), e que organizações (empresas, universidades, entre outras) que geralmente possuem redes conectadas à Internet pública, não seja comprometido (segurança) (KUROSE, 2010).

Segundo Tanenbaum e Wetherall (2011), a maior parte dos problemas de segurança é causada intencionalmente por partes maliciosas que de alguma forma tentam obter algum benefício, isto é, chamar atenção de alguém ou até mesmo prejudicar alguém. A tabela 1 lista alguns dos invasores mais comuns.

Tabela 1 - Algumas pessoas que podem causar problemas de segurança e os motivos para fazê-los.

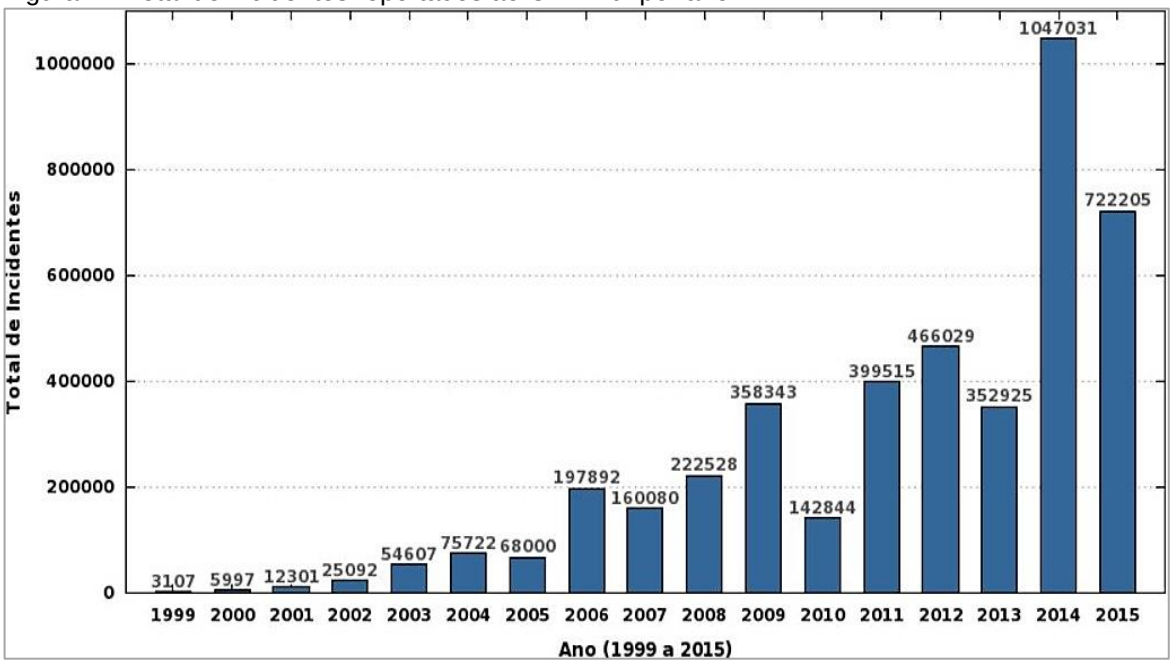
Adversário	Objetivo
Estudante	Divertir-se bisbilhotando as mensagens de correio eletrônico de outras pessoas
Hacker/Cracker	Testar o sistema de segurança de alguém; roubar dados
Executivo	Descobrir a estratégia de marketing do concorrente
Ex-funcionário	Vingar-se por ter sido demitido
Contador	Desviar dinheiro de uma empresa
Vigarista	Roubar números de cartão de crédito e vendê-los
Espião	Descobrir segredos militares ou industriais de um inimigo
Terrorista	Roubar segredos de armas bacteriológicas

Fonte: Tanenbaum e Wetherall (2011).

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), que é mantido pelo Comitê Gestor da Internet no Brasil (NIC.br), tem sido uma central de notificações de incidentes de segurança no Brasil. O Cert estabelece diretrizes estratégicas, promove estudos entre outras atribuições e objetivos (CERT.br, 2012b).

A figura 2 demonstra um desses estudos, registrando o total de incidentes ocorridos por ano, desde 1999 a 2015 (CERT.br, 2016).

Figura 2 - Total de incidentes reportados ao CERT.br por ano.



Fonte: Cert.br (2016).

Frente a estas estatísticas, observa-se um crescimento massivo no ano de 2014, correspondendo a 1.047.031 de incidentes no total, este número foi 197% maior

que o ano anterior que foram de 352.925, nos quais os incidentes foram de diferentes topologias. Os ataques DoS foram os campeões em crescimento. Eles somaram 223.935 registros, número 217 vezes maior que em 2013. O golpe consiste em tirar um serviço, computador ou rede de operação (NIC.br, 2016).

Ainda de acordo ao NIC.br, os ataques de negação de serviço foram os protagonistas no ano de 2014, especiamente os direcionados a servidores WEB. No geral, os ataques de força bruta foram os que mais cresceram neste ano, tendo como principais alvos os Sistemas de Gerenciamento de Conteúdo (*Content Management System* - CMS), tais como, o *WordPress* e o *Joomla*. Outros ataques também foram registrados como tentativas de fraude, varreduras e propagação de códigos maliciosos (NIC.br, 2015).

A *Verisign*, uma empresa especializada em nomes de domínio e segurança da Internet, complementa as estatísticas do Cert com o seu registro do ano 2015, onde registrou o maior nível de atividade de ataques desde que começou a registrar números. Vários setores (TI, comércio eletrônico, setor público, entre outros) foram alvos de ataques DoS. Os ataques de inundação de UDP foram os campeões (VERISIGN, 2015).

No anexo F, poderá ser consultado o percentual com mais detalhes, bem como as estatísticas de mitigação.

3.1 TIPOS DE ATAQUES MAIS COMUNS NO BRASIL

O Cert.br aponta como principais e mais comuns no Brasil, as ameaças (CERT, 2016):

a) ***worm*:** são programas maliciosos (*malware*), automatizados para propagação de códigos maliciosos na rede;
b) **WEB:** este tipo de ataque visa especificamente no comprometimento de servidores Web ou desfigurações de páginas de Internet;
c) **DoS (*Denial of Service*):** são ataques de negação de serviço, neste tipo de ataque o infrator utiliza um ou mais computadores (cluster) para retirar um determinado serviço do ar, ou seja, evitar que o tráfego válido chegue ao alvo do ataque;
d) **invasão:** caracterizam-se por todos ataques realizados com sucesso e que resultaram no acesso não autorizado há um computador ou rede;

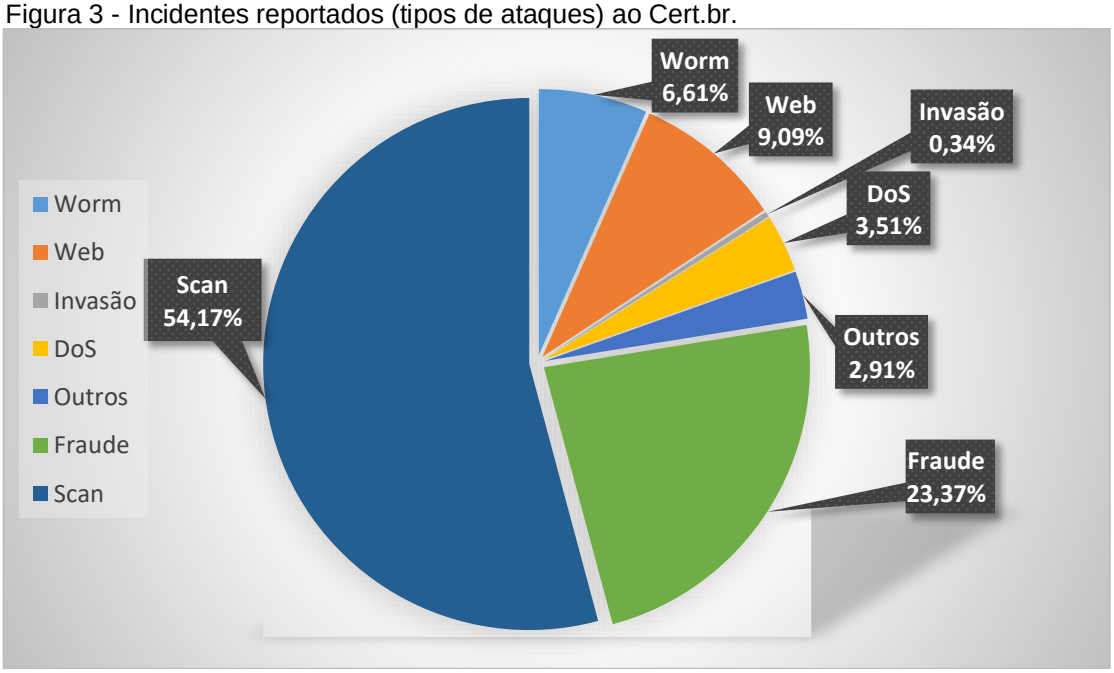
e) **fraude:** são todos incidentes que ocorrem com a intensão de obter algum tipo de vantagem;

f) ***scan:*** com a finalidade de obter potenciais alvos, e que estejam associados a possíveis vulnerabilidades, este tipo de ameaça, faz varreduras em redes de computadores identificando quais computadores e serviços estão ativos;

g) **outros:** encaixam-se em todas as notificações de incidentes que não pertençam as categorias anteriores.

A figura 3 representa os incidentes que foram reportados ao Cert.br do mês de janeiro a dezembro (CERT.br 2016).

Figura 3 - Incidentes reportados (tipos de ataques) ao Cert.br.



Fonte: Adaptado de Cert.br (2016).

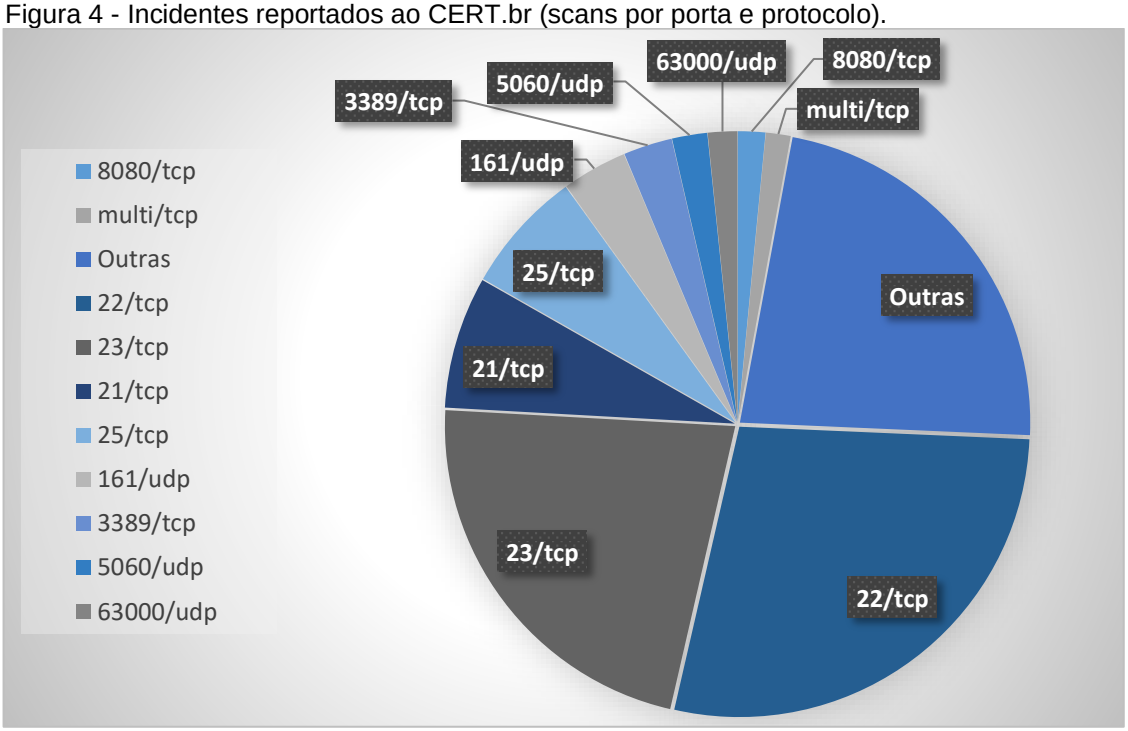
Antes de avançarmos a nossa atenção aos ataques DoS, de modo a saber os tipos de ataques DoS, como eles são feitos, entre outros pontos. É importante entender alguns protocolos que são utilizados e explorados para a realização destes ataques. Os protocolos abordados foram classificados de acordo o cenário proposto.

3.2 PROTOLOCOS DE COMUNICAÇÃO

Os protocolos de comunicação são responsáveis por realizar a comunicação entre duas ou mais entidades, tendo em vista a elaboração de algum serviço. São compostos por regras (de semântica e sintaxe) e formatos (estrutura de dados) (CARISSIMI; ROCHOL; GRANVILLE, 2009).

Acompanhe agora na figura 4, os incidentes de *scans*[6] por porta e protocolo reportados ao Cert no período de janeiro a dezembro de 2015. Não foram incluídos os scans realizados por *worms* (CERT.br, 2016).

Figura 4 - Incidentes reportados ao CERT.br (scans por porta e protocolo).



Fonte: Adaptado de Cert.br (2016).

Ao prosseguirmos com a análise das informações reportadas ao Cert na figura 4, observa-se claramente o índice elevado na utilização dos protocolos TCP e UDP para a realização de ataques.

Anteriormente, abordou-se sobre uma das características que definem os ataques DoS, o consumo excessivo de recursos. Todavia, não se havia mencionado

[6] Técnica para realizar buscas em redes de computadores, com o objetivo de capturar informações, como por exemplo, serviços e programas instalados. O termo scam (com m no final) tem um próposito diferente, geralmente são estratégias adotadas pelos cibercriminosos para enganar os usuários e obter vantagens financeiras (CERT.br, 2016).

até então uma outra caraterística peculiar, a de explorar vulnerabilidades e falhas na implementação de alguns protocolos. Sendo assim, abordaremos a seguir e resumidamente os protocolos que sofrem maior incidência dos ataques DoS.

3.2.1 Protocolo IP

O Protocolo de Internet (IP), foi concebido para interligar redes de comunicação (TANENBAUM; WETHERALL 2011).

De acordo ao seu documento oficial técnico (RFC 791), o protocolo é o responsável por prever a transmissão que ocorre entre os blocos (datagramas) a partir das suas fontes de destino, sendo identificados pelos endereços de comprimento fixo. Quando necessário, o protocolo ainda prevê a fragmentação e remontagem de longos datagramas (RFC 791, 1981, tradução nossa).

Segundo Fey (2016), existem atualmente duas versões deste protocolo, a 4ª versão que é ainda a mais utilizada (e conhecida por IPv4), e a 6ª versão (conhecida por IPv6) construída para substituir o IPv4.

Por fim, é importante mencionar que diferente do protocolo TCP, o protocolo IP apenas envia o pacote, ou melhor, em momento algum ele assume o controle da conexão entre a origem e o destino (SOUZA, 2007).

3.2.2 Protocolo TCP

O Protocolo de Controle de Transmissão, do inglês *Transmission Control Protocol (TCP)*, opera na camada de transporte[7] e é orientado a conexão confiável. Este protocolo está encarregue de controlar o fluxo, controlar os erros, e a sequêncialização e multiplexação do acesso ao nível inter-rede. A sua função consiste basicamente em fragmentar um fluxo de bytes[8] em mensagens e as entregar a camada inter-rede[9]. No decorrer do seu destino, o TCP restaura as mensagens recebidas em fluxo de bytes (FEY, 2016).

[7] Responsável por estabelecer a comunicação fim a fim entre à máquina de origem e destino (FEY, 2016).
[8] Unidade de informação digital, equivalente a 8 bits (GUIMARÃES; CABRAL, 2016).
[9] Uma arquitetura de rede que foi criada para resolver os passados problemas que existiam na implantação de redes de satélite e de enlaces de rádio. É também responsável pela entrega de pacotes (FEY, 2016).

3.2.3 Protocolo UDP

User Datagram Protocol (UDP), é um protocolo bastante simples e implementado na arquitetura TCP/IP. Diferente do que já foi visto, o protocolo UDP não é orientado a uma conexão confiável, nele, não há garantia na entrega de mensagens, não há controle de duplicações e também não há garantias sobre o ordenamento de pacotes. No entanto, o protocolo UDP adota um método eficiente para multiplexação de transmissões sobre o IP, além de incluir um conjunto de caracteres para verificar a confiabilidade da integridade dos dados através de *checksums*[10] (CARISSIMI; ROCHOL; GRANVILLE, 2009).

Em concordância, Souza (2007) explica que o protocolo UDP tende a ser mais rápido, justamente por não fornecer estas garantias. Seguindo ainda a sua linha de pensamento, o autor esclarece que diferente do UDP, o protocolo TCP adota uma série de mecanismos que permitem-lhe inicializar, preservar e encerrar a comunicação, negociar tamanhos de pacotes, identificar e retificar erros, evitar o congestionamento do fluxo e por fim, autorizar que os pacotes sejam retransmitidos.

3.2.4 Protocolo ICMP

Internet Control Message Protocol (ICMP), tem a função de comunicar ao transmissor a ocorrência de erros durante o processamento de algum pacote no roteador (TANENBAUM; WETHERRALL, 2011).

Sendo assim, o ICMP trabalha com cinco tipos principais de mensagens de erros: (1) destino não alcançável, (2), tempo excedido (3), problema de parâmetro (4), redirecionamento, e (5) pedido e respostas de informações (CARISSIMI; ROCHOL; GRANVILLE, 2009, tradução nossa).

[10] É o conjunto de dados para conferir a integridade de um ficheiro baixado, sendo que são obtidos a partir de uma soma de verificação (CAMBRIDGE, 2016).

3.2.5 Protocolo SSDP e NTP

Uma nova pesquisa feita em *Las Vegas* no evento da *Black Hat* [11] 2016, apontou que os ataques DoS estão mais propensos a utilizar o protocolo SSDP em relação ao NTP. Na pesquisa, ainda foi apontado que os atacantes estão a mudar as estratégias de seus ataques e, que existem novos serviços que podem ser contratados online para aqueles que procuram alcançar ataques do gênero. Normalmente estes serviços oferecem uma boa estrutura de ataque, uma vez que recebem investimentos altos e cobram pelos serviços (BLACK HAT; WU, 2016, tradução nossa).

Simple Service Discovery Protocol (SSDP), é um protocolo baseado no UDP. Este protocolo é uma técnica subjacente para o amplamente utilizado e conhecido por *Universal Plug and Play (UPnP).* Utilizamos este protocolo no nosso dia a dia, e praticamente em todo nosso ambiente, seja em dispositivos de armazenamento, de imagem, entre outros. Fato é, que acabamos por muitas vezes a não nos apercebemos da sua existência. Do outro lado, os atacantes aproveitam-se desse descuido e fazem uso do protocolo SSDP para ampliar os ataques DDoS (BEAVER, 2015, tradução nossa).

Network Time Protocol (NTP), é outro protocolo baseado no UDP e sobre a porta 123, é utilizado para manter o relógio dos computadores de uma rede sincronizados. Para que isto seja possível, o NTP utiliza o *Coordinated Universal Time (UTC)*[12]*.* O NTP trabalha com o modelo cliente-servidor, ou seja, o cliente NTP inicializa uma troca de solicitação de tempo com o servidor. O resultado desta troca permite o cliente calcular o atraso de uma ligação e, consequentemente ajustar o seu relógio para corresponder com o relógio do servidor (ROUSE, 2007a; HELLER, 2016, tradução nossa).

O protocolo NTP foi desenvolvido sem levar em consideração alguns aspetos de segurança, o que resultou na descoberta de algumas vulnerabilidades e que permitiu que cibercriminosos tirassem proveito desta situação. Na prática, a

[11] Evento mais técnico e relevante relacionado à segurança da informação global no mundo. Por mais de 18 anos tem fornecido a comunidade de segurança pesquisas sobre a segurança da informação (BLACK HAT, 2016, tradução nossa).
[12] Tempo Universal Coordenado, é um padrão comum em todo mundo. É utilizado para calcular todas outras zonas horárias (ROUSE, 2008).

vulnerabilidade reside na quantidade de dados que o NTP envia e recebe, sendo que a quantidade enviada é maior que a quantidade recebida, um ambiente que se mostra adequado para os ataques DDoS de amplificação (ASHFORD, 2014, tradução nossa).

Apesar da utilização destes protocolos para amplificar ataques DoS, esta não vem a ser a maior preocupação que as empresas precisam ter, é o que aponta o relatório de uma das fornecedoras de proteção contra-ataques DoS, à *Incapsula Inc*. No relatório, a empresa adverte e solicita especial atenção para os ataques DoS do tipo *SYN Floods*, estes tipos de ataques podem causar muito mais danos que os demais usados (BLEVINS, 2014 apud INCAPSULA INC, 2014, tradução nossa).

Uma vez esclarecido a influência de alguns protocolos que estão sobre os ataques DoS, estamos aptos para dar continuidade e entendermos mais sobre eles.

Desta forma, aborda-se a seguir os ataques de negação de serviço, dando ênfase ao tipo de ataque DoS proposto (*SYN Flood*).

3.3 ATAQUES DE NEGAÇÂO DE SERVIÇO

Negação de Serviço, do inglês *Denial of Service* (DoS) é uma técnica que consiste em retirar de operação um serviço, um computador, ou uma rede conectada à Internet. Normalmente, o atacante utiliza um equipamento que já esteja conectado a esta rede. É o que diz o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br, 2016).

Ataques de negação de serviço representam atualmente uma séria ameaça para o correto funcionamento da Internet, e nos últimos anos, o tráfego malicioso gerado por esses ataques só vem se multiplicando. Os mecanismos de defesa tradicionais para ataques de negação de serviço seguem uma abordagem reativa, ou seja, só depois que os ataques desse tipo causam enormes prejuízos é que se procura novos mecanismos de defesa que estejam à altura. Esta abordagem não é aceitável levando em consideração o grau de risco que esses tipos de ataque representam (PIEDRAHITA, 2014).

Quando utilizado de maneira coordenada e distribuída, ou seja, quando um conjunto de equipamentos é utilizado para a realização do ataque, recebe o nome de Ataque Distribuído de Negação de Serviço, do inglês, *Distributed Denial of Service* (DDoS) (CERT.br, 2016).

Basta (2014) explica que os principais alvos desses ataques são os servidores web, servidores de aplicativos e links de comunicação. O propósito dos ataques DoS é negar o acesso ao tráfego legítimo, interrompendo e danificando conexões entre computadores, impossibilitando que usuários finais acessem os serviços de uma máquina, alterando as configurações do sistema e, em alguns casos, destruindo os componentes da rede física. Ataques de negação são capazes de desativar uma rede, destruir dados, e levar a perdas financeiras bastante significativas.

O Cymru (2010, tradução nossa) alerta que qualquer rede, equipamento ou sistema que esteja acessível pela Internet pode ser alvo de um ataque DDoS e, estando mal configurado, infetado ou inválido, pode ser manipulado e utilizado para gerar um ataque a outras vítimas. Setores como, provedores, jogos, notícias, bancos, comércio eletrônico, governo, indústria e partidos políticos já foram alvos de ataques DDoS.

3.3.1 Breve história

Ataques de negação de serviço tem sido uma escolha para os cibercriminosos desde os primórdios da Internet (HOFFMAN, 2013, tradução nossa).

A pesquisa conduzida por Sauter (2014, tradução nossa), relata que o ataque mais antigo e conhecido aconteceu em 1995, durou cerca de uma hora e foi realizado pela rede *strano* (um coletivo italiano) que lançou o ataque com a finalidade de protesto contra a política nuclear do governo francês. Nessa época, para se realizar um ataque os participantes necessitavam estar presentes em seus computadores, pois o custo de Internet era relativamente alto, e os ataques não deveriam durar muito tempo.

Já o estudo conduzido pela analista Ponteves (2013), aponta como o primeiro ataque distribuído de negação em grande escala no servidor IRC da Universidade de Minnesota em 1999. No total, 227 sistemas foram afetados inutilizando o servidor por dois dias. De 2000 adiante, os alvos foram sites populares como o *Yahoo*, *eBay*, CNN, *Amazon.com*, ZDNet.com ficaram paralisados durante horas, só o Yahoo sofreu uma perda de U$ 500.000 durante as três horas que esteve inacessível. Nos últimos anos, os atacantes têm aumentando o volume de ataques bem como as técnicas utilizadas.

Sauter (2014, tradução nossa) explica que ataques de negação de serviço têm parte de sua origem e ligação, há protestos e movimentos de ativistas que eram contra o encontro da Organização Mundial do Comércio (OMC)[13].

3.3.2 Causas de ataques DoS

Ataques DoS acontecem devido as restrições que as infraestruturas possuem, ou seja, algumas vulnerabilidades não podem ser resolvidas devido ao limite de largura de banda, ou de conexões ativas comum a todos os dispositivos de uma rede, sejam eles físicos ou de *software*. Por exemplo, se um servidor web possui uma capacidade de aceitar mil pedidos por segundo, então o milésimo primeiro pedido será negado. É comum para as organizações ao ultrapassar a capacidade do seu servidor, realizar atualizações ou até mesmo trocar por outro *software* que aceite mais pedidos. Todavia, a plataforma atual de *hardware* pode não suportar esse novo *software*, exigindo assim *upgrades* de CPU e de memórias RAM (BASTA, 2014).

Outras várias razões podem servir de motivação para que ataques de negação de serviço aconteçam. Por exemplo, situações de extorsão, lucro financeiro, trocas, reconhecimento, visibilidade, regimes opressivos, guerras, rivalidade pessoal, hacktivismo[14], entre outros (ZELTSER, 2015, tradução nossa).

Por fim, Basta (2009) reforça que as organizações devem encontrar um equilíbrio entre risco e benefício quando dimensionam a tecnologia usada para apoiar suas funções de negócio. Tal como o risco, o tamanho do impacto que um ataque DoS pode gerar, são elementos importantes na tomada de decisão. Para uma organização em particular, mesmo que a probabilidade de sofrer um ataque desse tipo seja extremamente baixa, o impacto potencial que um ataque deste tipo poderia causar poderia compensar o dinheiro gasto para atualizar a tecnologia, garantindo ser possível lidar com a situação.

---

[13] *Worls Trade Organization* (WTO) ou Organização Mundial do Comércio (OMC), tradução literal para o português, conhecidas também como batalha de Seattle ou ainda N-30, foram manifestações ocorridas em 30 de novembro de 1999 contra a reunião da OMC. Tendo como objetivo protestar contra o avanço das políticas neoliberais, as negociações da OMC, a manutenção dos direitos trabalhistas e ao capitalismo global (Wikipédia, 2014).

[14] *Hacker* ou *cracker* motivado pelo patriotismo, nacionalismo ou outra crença profunda (BASTA, 2014).

3.3.3 Tipos de ataques DoS

Basicamente existem cinco tipos de ataques de negação de serviço: (1) ataques evitáveis, (2) não evitáveis, (3) ataques baseados em *software* por inundação, (4) ataques isolados e (5) distribuídos (BASTA, 2014).

a) **DoS evitável**: ocorrem quando o sistema é projetado pelo administrador de redes para executar vários serviços sem ter em conta a sua limitação, seja em nível de rede ou de aplicação. Por exemplo, o administrador projeta um sistema baseado em VoIP (voz sobre IP) com 120 telefones, estimando em média um uso de 20% do tempo, sem medir a capacidade de uso, dessa forma, admite que a capacidade do sistema seja suficiente somente para acomodar um em cada cinco usuários a cada momento. Isso funciona bem tanto na teoria como na prática, até que, seja convocada uma audioconferência e mais de 30% dos funcionários da empresa participem. Como o sistema foi projetado com apenas 20% de uso, ao exceder esse limite o sistema vai falhar: as chamadas serão derrubadas e haverá várias ordens de serviço de manutenção. A esta perda de recursos disponíveis resulta a um tipo de DoS;

b) **DoS não evitável**: já sugestivo e diferente do primeiro, o administrador não pode o evitar que aconteça, visto que o administrador do sistema não pode o prever, portanto, não está preparado. Por exemplo, o administrador recebe um aviso que uma das impressoras não está a funcionar e ao se conectar ao servidor, verifica que há uma grande quantidade de trabalhos em fila e que não podem ser impressos por estarem mal formatados. Eles consomem todo o espaço disponível em disco, negando assim o acesso a outros usuários. Nesse caso, é bem provável que esteja a acontecer um ataque ao servidor de impressão, resultando em uma negação de serviço;

c) **ataques por inundação**: de maneira geral, processos em execução, seja em computadores ou dispositivos de rede, demandam de largura de banda e espaço de memória e em disco. Também necessitam de estruturas de dados e tempo de CPU o seu correto funcionamento.

Sendo que os dispositivos vêm de fábrica programados com uma capacidade máxima de processamento de pacotes. Ataques de inundação consomem esses recursos limitados, sobrecarregando assim a rede e negando recursos a usuários legítimos;

d) **ataques isolados**: provém de uma única fonte e podem ser facilmente bloqueados a partir de um *firewall*;

e) **ataques distribuídos**: este tipo de ataque é gerado por várias fontes simultaneamente. Ataques DDoS são mais difíceis de serem bloqueados com listas de controle de acesso (ACL) ou regras de *firewall*.

Segundo a taxonomia de ataques DoS/DDoS classificada por Riorey (2015, tradução nossa), os ataques de inundação de pacotes podem ser:

a) **SYN *Flood* (baseado no protocolo TCP):** neste tipo de ataque, o servidor vítima recebe centenas e centenas de requisições de abertura de conexão SYN, o atacante pode falsificar os endereços de IPs para dificultar o bloqueio do ataque;

b) **SYN-ACK-*Flood* (baseado no protocolo TCP):** o servidor vítima passa a receber centenas e centenas de requisições de abertura de conexão SYN-ACK a partir de endereços falsificados;

c) **ACK & *Push* ACK Flood (baseado no protocolo TCP):** o servidor vítima passa a receber centenas e centenas de pacotes do tipo ACK falsificados, onde a taxa de envio pertence a uma qualquer outra sessão legítima dentro da lista de conexão ao servidor;

d) ***Fragmented* ACK (baseado no protocolo TCP):** este tipo de ataque consiste em consumir a maior quantidade de banda possível, é possível definir para cada pacote até 1500 bytes;

e) **RST ou FIN *FLOOD* (baseado no protocolo TCP):** um servidor vítima passa a receber centenas e centenas de pacotes do tipo RST ou FIN falsificados, onde a taxa de envio não pertence a qualquer outra sessão legítima dentro da lista de conexão do servidor;

f) ***Synonymous* IP (baseado no protocolo TCP):** são enviados pacotes do tipo TCP-SYN falsificados em uma taxa elevada para o servidor vítima, estes pacotes contém a informação do servidor descrita como: endereço de IP de origem e de destino;

g) **UDP *Flood* (baseado no protocolo UDP):** são enviados milhares de pacotes falsificados do tipo UDP a partir de centenas de fontes de Ips de origem, normalmente neste tipo de ataque, as taxas de envio são muito altas;

h) **UDP *Fragmentation* (baseado no protocolo UDP):** é uma variante do ataque do tipo UDP Flood, contudo, o servidor vítima pode receber uma variação alta ou baixa de pacotes num tamanho de até 1500 bytes;

i) **DNS *Flood* (baseado no protocolo UDP):** são utilizadas diversas fontes de origem para falsificar pacotes DNS a taxas altas, todavia, o servidor vítima entende que são requisções válidas;

j) **VoIP *Flood* (baseado no protocolo UDP):** o servidor vítima recebe centenas e centenas de pacotes do tipo VoIP, que são originados a partir de diversas fontes de origem e com taxas altas;

k) ***Media Data Flood* (baseado no protocolo UDP):** outra variante do UDP Flood, no entanto, neste tipo de ataque os pacotes apresentam como tipo de ficheiro dados de mídea;

l) ***Non-Spoofed* UDP *Flood* (baseado no protocolo UDP):** nesta variante, os pacotes não são falsificados e são enviados em taxas altas;

m) **ICMP *Flood* (baseado no protocolo ICMP):** são enviados diversos pacotes falsificados ICMP, de diferentes fontes de origem e com taxas altas para o servidor vítima;

n) **ICMP *Fragmentation* (baseado no protocolo ICMP):** variante do ICMP Flood, o servidor vítima recebe pacotes fragmentados com tamanho de 1500 bytes e que não podem ser remontados;

o) **Ping *Flood* (baseado no protocolo ICMP):** são enviados para o servidor vítima ICMP echo requests (ping), originados a partir de diversas fontes e com taxas altas.

Basta (2014) acrescenta os ataques por inundação de ping, ping da morte e o de serviço DNS. Ataques de inundação podem ocorrer das seguintes maneiras:

a) quando um elevado número de solicitações de conexão é enviado;

b) a partir do momento em que uma grande quantidade de banda é consumida;

c) quando os recursos das vítimas são usados contra elas próprias;

d) quando se dá a utilização de recursos de outros contra as vítimas.

3.3.3.1 Ataque DoS SYN Flood

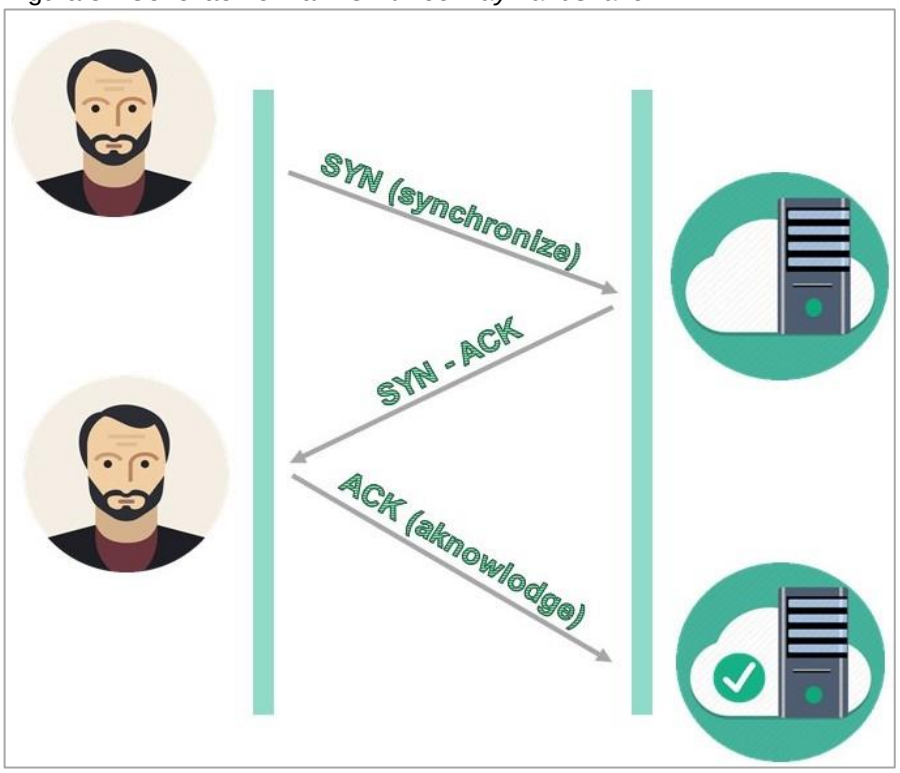
Para entendermos propriamente o comportamento de um ataque do tipo SYN Flood, precisamos antes compreender como funciona o aperto de mão em três etapas, do inglês *Three-Way HandShake* TCP/IP. De modo simplificado, para que uma conexão seja aberta e possa ser realizada no modelo cliente-servidor, é necessário que ambos se apresentem antes.

Em uma conexão normal do modelo cliente-servidor, o cliente tenta estabelecer uma conexão TCP e espera uma resposta do servidor. Durante essa comunicação, há uma troca de um conjunto de mensagens, nomeadamente (CERT.org, 2000, tradução nossa):

a) o cliente solicita uma conexão com o envio de uma mensagem SYN (*synchronize*);
b) por sua vez, este responde a sua solicitação enviando uma mensagem SYN-ACK (*acknowledge*);
c) ao final, o cliente finaliza a conexão com o envio de uma mensagem de confirmação ACK.

Diante do contexto acima, a conexão é estabelecida e aberta entre o cliente e servidor, ambos passam então a estar apresentados, e podem trocar os dados correspondentes ao serviço (figura 5) (CERT.org, 2000, tradução nossa).

Figura 5 - Conexão normal TCP *three-way handshake*.



Fonte: Do autor (2016).

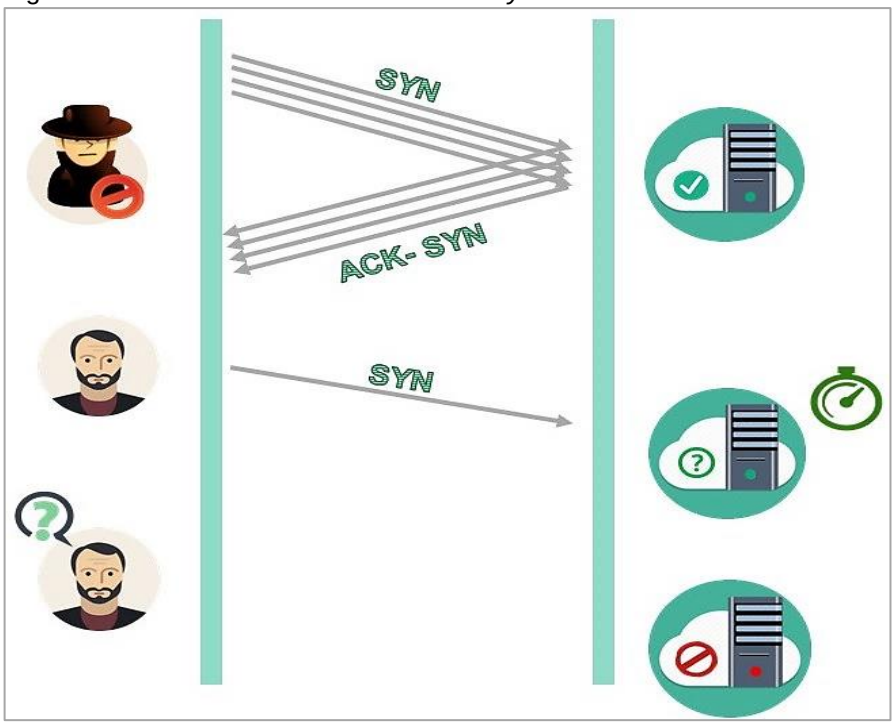
Consideremos agora uma conexão anormal, ou seja, uma conexão que esteja sobre a influência de um atacante que utiliza como forma de ataque DoS, o *SYN Flood*.

O Professor Mestre em Ciência da Computação pela Universidade Federal do Rio Grande do Sul (UFRGS) Schlemer (2007), aponta em um dos seus artigos um fator muito importante. Como o protocolo TCP é confiável, quando o servidor responde às solicitações de SYN enviadas pelo cliente, ele já passa alocar os recursos de *hardware* para atender à solicitação. Estes recursos não sou poucos, pois envolvem *buffers* de envio e recebimento, controle de números, recursos de memória, recursos de processamento, entre outros.

O que acontece num ataque SYN Flood vai de encontro a explicação feita pelo professor. O ataque induz o cliente a solicitar repetidamente mensagens SYN, em uma conexão normal este cliente deveria confirmar com uma mensagem SYN-ACK, mas em vez disso ele não as responde. Para dificultar ainda mais o processo, o atacante combina vários IPs falsos e direciona o ataque para várias portas, o servidor entende como solicitações válidas e aloca os recursos esperando a sua confirmação. Obviamente esta confirmação nunca é feita, e o servidor torna-se parcialmente ou completamente inoperante (BLEVINS, 2014, tradução nossa).

Na figura 6, é esclarecido este contexto, exibindo uma conexão anormal *handshake* TCP/IP.

Figura 6 - Conexão anormal TCP *three-way handshake*.



Fonte: Do autor (2016).

Há que se mencionar um fator importante, os *firewalls* comuns, ao contrário do que é abordado, não podem resolver este problema limitando apenas o tempo das conexões *SYN*, a solução até impediria que ocorresse um *SYN Flood*, mas não uma negação de serviço, que é o principal objetivo do criminoso, pois bastaria que o atacante excedesse o tempo configurado para que o próprio *firewall* instalado retirasse o serviço do ar, não aceitando mais usuários, sendo estes legítimos ou não (SCHLEMER, 2007).

A seguir, dá-se continuidade a outros conceitos relacionados aos ataques DoS.

3.3.4 Tipos de ataques DDoS

Levando em consideração que existem diferentes tipos de ataques DDoS, as organizações devem planejar atentamente e adequadamente as ações a serem tomadas. Basicamente existem três tipos de ataques DDoS (CERT.br, 2016):

a) **ataques à camada de aplicação**: tendem a ser mais difíceis de ser detectados, pois podem ser facilmente confundidos com problemas de implementação. A *CloudFlare* (2016, tradução nossa) acrescenta que a maioria dos ataques DDoS ocorrem nas camadas de rede e transporte de um sistema de comunicações. Estas camadas são representadas como camadas 3 e 4 no modelo OSI. A camada de transporte é a responsável pela transferência transparente de dados entre emissor e receptor, para tal, pode fazer uso de alguns de seus protocolos (por exemplo, TCP ou UDP). Ataques dirigidos a estas camadas são projetados para inundar uma interface de rede com tráfego malicioso, com a finalidade de dominar seus recursos e negar a capacidade de resposta do tráfego legítimo. Os ataques à camada de aplicação nas camadas de rede e transporte são difíceis, se não impossíveis de serem mitigados com soluções locais. O Cert.br (2016), completa que é comum que ataques deste tipo procurem explorar características específicas de uma aplicação ou serviço (camada 7) de tal maneira a saturar recursos; a exceder o número máximo de requisições de um servidor ou um sistema gerenciador de banco de dados (SGBD); há consultas que demandem muito processamento. HTTP GET, HTTP POST, VoIP (SIP *INVITE Flood*) e *Slow Read* DDoS são exemplos destes tipos de ataques;
b) **ataques de exaustão de recursos de *hardware***: procuram consumir a capacidade de equipamentos e estropiar seus recursos. Por exemplo, em roteadores, tentam consumir recursos como CPU, memória e a capacidade de encaminhamento de pacotes por segundo (pps), já em *firewalls* e IPSs visam consumir a capacidade da tabela de estado de conexões, impossibilitando assim que novas conexões sejam estabelecidas. Fragmentação e TCP *SYN Flood* são alguns exemplos;
c) **ataques volumétricos**: procuram extrapolar a banda disponível enviando à vítima uma enorme quantidade de tráfego. Para conseguir esse enorme volume, os atacantes fazem uso de *botnets*, máquinas com bastante banda, máquinas com pouca banda, mas em uma grande quantidade, ou ainda, exploram características específicas de serviços

UDP que possibilitam a amplificação de tráfego. DRDoS é um exemplo deste ataque (CERT.br, 2016).

De acordo ao Cert.br (2015), a facilidade em que se pode ter acesso a grande quantidade de ferramentas disponíveis na Internet, sejam elas gratuitas ou a preços cada vez mais acessíveis, permite que qualquer pessoa possa realizar ataques de negação. De forma geral os ataques ocorrem das seguintes formas:

a) por um aglomerado de *botnets* em equipamentos infetados, mal configurados ou inválidos, como computadores pessoais, servidores WEB, dispositivos móveis, roteadores, câmeras, Wi-Fi, modems banda larga, etc. Sendo que estes dispositivos passam a receber comandos remotamente do controlador;
b) sobre a exploração de vulnerabilidades em serviços e aplicações, geralmente causas por erros de configuração e programação;
c) através de usuários que voluntariamente disponibilizam seus computadores para participar de ataques através de sites específicos que disponibilizam ferramentas como HOIC, LOIC, *RUDY* e *Slowloris*. Esses ataques passam a ser coordenados por redes sociais e canais de IRC, entre outros meios;
d) pelo meio de aplicações WEB específicas chamadas de boters, IP *Stressers* ou DDoS, ofertados às vezes como ferramentas legítimas de carga, mas que na verdade são ferramentas utilizadas para ataques via boters ou máquinas alugadas para este fim;
e) sobre a exploração de serviços de Internet como, DNS, NTP, SSDP, e *CHARGEN*, que permitem altas taxas de amplificação de pacotes. A técnica consiste em forjar o IP da vítima e consumir uma quantidade considerável de banda de rede. Vários equipamentos, como CPEs, muitas das vezes possuem esse serviço ativado de fábrica.

Para complementar os esclarecimentos acima retratados, o anexo E ilustra o comportamento de um ataque DDoS.

3.3.5 Diferença de ataques DoS e DDoS

Ataques DoS, acontecem quando o atacante utiliza uma única conexão de Internet, seja para explorar vulnerabilidades de *software* ou inundar o alvo com falsas

solicitações, na maioria das vezes em tentativas de esgotar recursos de um servidor (por exemplo, RAM e CPU). Outra diferença é dada pela forma de execução, ataques DoS são gerados a partir de scripts *homebrewed*[15] e ferramentas DoS (por exemplo, *Low Orbit Ion Canon, Hping,* T50, entre outras) (INCAPSULA, 2016, tradução nossa).

Já os ataques DDoS ocorrem a partir de várias conexões e múltiplos dispositivos distribuídos pela Internet. Ataques DDoS são de difícil mitigação pelo fato de gerarem um volume de tráfego muito alto. Ataques DDoS são executados a partir de um aglomerado de *botnets*[16] conectados (celulares, computadores, roteadores, etc.) infetados com algum *malware*[17] que permite ao invasor controlo remoto (INCAPSULA, 2016, tradução nossa).

3.3.6 Métodos de prevenção de ataques DoS e DDoS

Pascucci (2013, tradução nossa) especialista e pesquisador em segurança da informação, sugere três técnicas para prevenção de ataques DoS e DDoS:

a) **1ª sugestão**: determinar os recursos existentes e avaliá-los de modo a saber se podem limitar ou reduzir alguns ataques. Por exemplo, limitações de tráfego em *firewall* ou em *load balancers*, criação de procedimentos para contatar o ISP, realização de bloqueios geográficos de IP, configuração de alertas de aumento de tráfego, condições de cortar ou remover algum serviço que atue na da camada de aplicação e a implementação de um processo de resposta a incidentes de ataques DoS;

b) **2ª sugestão**: implementação de aparelhos de fornecedores como a *Arbor Networks*, *Fortinet*, *Check Point*, entre outros, que ajudam a prevenir ataques de negação. No entanto, o especialista destaca que apesar de serem aparelhos sofisticados, são aparelhos caros ou com assinaturas altas, e exigem treinamentos constantes;

c) **3ª sugestão**: o autor sublinha esta última sugestão como sendo a com maior potencial e capacidade para absorver ataques DoS. A

[15] Feitos em casa (tradução literal para o português).
[16] Rede de computadores comprometidos (zumbis) que são usados ou vendidos para uso em atividades ilegais ou maliciosas (BASTA, 2014).
[17] Código malicioso (CERT.br, 2012a).

solução consiste no uso de uma rede de distribuição de conteúdo (CDN) para filtrar o tráfego malicioso antes mesmo de chegar aos servidores locais.

De acordo ao Cert (2016), a segurança de uma rede depende proporcionalmente da segurança dos demais setores que formam à Internet. Desta forma, recomenda quatro medidas que devem ser tomadas de modo a reduzir a incidência de ataques DoS:

a) **usuários finais:** precisam ter bastante atenção para não serem voluntareamente utilizados remotamente como robõs para ampliarem ataques DoS. O uso de técnicas como a engenharia social, levam usuários a pensarem que estão a contribuir com alguma causa, quando na verdade estão a ser enganados ao permitirem acesso às suas máquinas para cibercriminosos. Normalmente, estes usuários são atraídos por meio da instalação de ferramentas ou por portais especifícos. Uma política adequada de segurança e programas de conscientização, ajudam os usuários a estar a par das ameaças existentes e das medidas que podem ser tomadas;
b) **desenvolvedores de aplicações Web:** junto com os links de comunicação, fazem parte dos princípais alvos dos ataques DoS, isto porque possuem capacidades muito altas de processamento, banda e armazenamento (ambientes bem estruturados). Para os atacantes, são os ambientes perfeitos para instalarem suas ferramentas DoS;
c) **administradores de redes:** podem melhorar o cenário de ataques DoS e de ameaças em geral, seguindo e implementando à risca as boas práticas de segurança. Devem ainda adotar uma abordagem proativa para algumas situações. Recomenda-se também, a participarem voluntareamente ao notificarem sobre incidentes ocorridos aos orgãos responsáveis pelos estudos e tratamentos de incidentes (Cert, Nic, entre outros). Outras boas práticas como: (1ª) atualizar os equipamentos e serviços (SGDB, módulos e plugins), (2ª) configurar corretamente serviços e aplicações, (3ª) monitorar logs, (4ª) monitorar todo tráfego de entrada e saída, (5ª) ser criterioso, (6ª) controle de permissões e privilégios de usuários, (7ª) elaboração de políticas de segurança adequadas, (8ª) campanhas de sensibilização, (9ª) possuir

funcionários qualificados, e (10ª) acompanhar as tendências de ataques e vulnerabilidades, bem como, novas soluções de segurança, permitem reduzir o número de incidentes e a fortalecer a estrutura de segurança do ambiente;

d) **provedores de conectividade:** da mesma forma, devem seguir as boas práticas de segurança, visto que ao implementá-las fortalecem não só à sua infraestrutura, mas como também a de seus clientes. Algumas práticas como: (1) habilitar o filtro antispoofing, (2) proteger os CPEs dos clientes, (3) e configurar adequadamente os serviços, principalmente os com base nos protocolos DNS, NTP, SNMP, SSDP, UDP, TCP/IP auxilam na prevenção de ataques DoS.

Na eventualidade de acontecer o ataque, o Cert.br recomenda oito ações a serem tomadas (CERT.br, 2016):

a) documentar o incidente, descrevendo todas ações que contribuíram para o êxito do ataque;
b) rever a abordagem adotada pelo departamento de TI, observando o que poderia ter sido feito antes do ataque, ou seja, uma adoção proativa;
c) manter a lista de contatos de prestadores de serviços sempre atualizadas;
d) rever as cláusulas dos contratos;
e) na ausência de uma contramedidade de mitigação na *cloud,* aperfeiçoar as etapas de preparação, detecção, análise e mitigação de ataques DoS;
f) verificar se existem outras áreas vulneráveis que permitam que incidentes de outras topologias aconteçam;
g) analisar cuidadosamente os *logs* durante o ataque, de modo a extrair o máximo de informações que possam ser úteis;
h) notificar voluntareamente instituições que de alguma forma estejam a ser utilizadas para gerarção do tráfego de ataque, todavia, esta ação só pode ser tomada quando se consegue identificar a origem do ataque.

Empresas como *Maxihost*, *CloudFlare*, *Incapsula, Akamai Tecnologies*, *Verisign*, *Nexusguard*, *Riorey,* entre outras, já oferecem o serviço de filtrar todo tráfego

malicioso através de suas próprias redes antes que ele atinja seus clientes (PASCUCCI, 2013, tradução nossa). Vale reiterar, que é esta a solução que esta pesquisa oferece.

3.4 POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO NAS EMPRESAS

A escolha das decisões corretas nunca é uma tarefa fácil, são as decisões que um administrador segue ou deixa de seguir, pertinente a segurança, que irão determinar quão segura ou insegura é a sua rede, quantas funcionalidades ela irá oferecer, e qual será o nível de clareza para utilizá-las. Entretanto, não é uma tarefa fácil tomar as decisões corretas sobre segurança, sem antes determinar quais as melhores técnicas de segurança, é o que diz o guia de configuração de segurança RFC 2196 (FRASER,1997, tradução nossa).

Uma política tem um papel fundamental e, sua importância assemelha-se à Constituição Federal de um país, sua finalidade é de oferecer orientação e suporte às ações de gestão de segurança.

Durante a criação do conjunto de políticas de segurança da informação nas organizações, estas precisam ser avaliadas, aprovadas pela administração, publicadas e comunicadas para os empregados e partes externas relevantes (FERNANDES; ABREU, 2014).

Convém que a direção da empresa procure estabelecer uma política que venha a ser clara, e que esteja alinhavada com os objetivos do negócio. Deve demonstrar fundamento e compromisso com a segurança da informação, mediante à publicação e manutenção de uma política de segurança da informação para toda a organização (ABNT NBR ISO/IEC 27005, 2011).

4 *CLOUD COMPUTING*

A Computação em Nuvem, do inglês *Cloud Computing*, está sendo responsável por uma das maiores revoluções nos últimos anos na área de Tecnologia da Informação (TI) (OPUS SOFTWARE, 2015).

A *cloud computing* é um novo modelo de negócio que cada vez mais cresce e ganha espaço no mercado de TI, seu modelo garante a entrega de diferentes serviços, dos quais, a segurança foi o foco deste trabalho. *Intrusion Detection System (IDS)*, *Intrusion Prevention System (IPS)* e *Content Delivery Network (CDN),* são mecanismos eficazes para detecção e prevenção de ataques de negação de serviço (ALQAHTANI; BALUSHI; JOHN, 2014, tradução nossa).

O estudo conduzido por Turban e Volonino (2013), define que a *cloud computing* é uma computação que tem como base à Internet, onde recursos são compartilhados (como discos de armazenamento) e aplicativos são oferecidos ao computador ou a outros dispositivos por demanda, como uma utilidade pública. Os autores seguem com a sua linha de pensamento e do mesmo modo que (SOUSA NETO, 2016), relacionam a *cloud* com a eletricidade nas empresas, uma utilidade que têm disponível conforme a demanda e pagam com base no uso. As empresas não geram sua própria energia, elas obtêm de fornecedores, neste caso, as companhias de energia.

4.1 MODELOS DE IMPLANTAÇÃO NA *CLOUD COMPUTING*

Considerada como a mudança natural dos modelos anteriores e como a nova arquitetura de TI, a *cloud computing* permitiu mudar o conceito de obtenção as novas soluções de TI. O surgimento do modelo, pagamento pelo uso, do inglês *pay-per-use*. Introduziu o conceito de pagar apenas pelos recursos que são utilizados e não por toda infraestrutura, fora que se adequa a necessidade do cliente (VERAS, 2013).

Ao se implantar uma *cloud computing,* se deve avaliar os quatro critérios de acesso que a constituem, *Cloud* Privada, *Cloud* Pública, *Cloud* Híbrida e *Cloud* Comunitária.

4.1.1 *Cloud* privada

A infraestrutura de uma *Cloud* Privada, do inglês *Private Cloud* é exclusiva para uso de uma única organização e pode incluir vários outros consumidores, por exemplo, outras subdivisões da empresa. Pode ser de propriedade, gerenciado e operado pela própria organização, terceiros, ou a combinação de ambos, e não necessariamente precisa existir no local (NIST, 2013, tradução nossa).

Em comparação aos demais modelos de implantação, a *cloud* privada é a que pode oferecer menos riscos, face a sua natureza privada. No entanto, exige um gerenciamento interno que resulta na diminuição e economia de recursos. Fora estar ligada diretamente aos processos corporativos, o que dificulta em termos de automação de tarefas, tais como, atualizações (CASTRO; SOUSA, 2011).

A implantação deste modelo implica em políticas de acesso e técnicas em nível de gerenciamento aos seus serviços, exigindo técnicas em nível de gerenciamento de redes, configurações dos provedores de serviços e a utilização de tecnologias de autenticação e autorização (NIST, 2011, tradução nossa).

4.1.2 *Cloud* pública

A *Cloud* Pública, do inglês *Public Cloud* possui uma infraestrutura aberta para o público em geral. O seu acesso exige que o usuário ou a organização saibam a localização do serviço. Pode ser de propriedade, gerenciado e operados pela própria organização, acadêmicos, organizações governamentais, ou ainda na combinação deles e, deve existir nas instalações do provedor *cloud* (NIST, 2013, tradução nossa).

Neste modelo de implantação não podem ser aplicadas restrições de acesso no que se refere ao gerenciamento de redes, e menos ainda, a técnicas de autenticação e autorização (CASTRO; SOUSA, 2011).

O modelo concede às organizações uma redução de custos em escala, já que compartilha os recursos. Em contrapartida, os dados são salvos em locais desconhecidos e de difícil acesso, o que limita a customização relacionada a segurança das informações, SLAs e políticas de acesso (CASTRO; SOUSA, 2011).

Infraestruturas de *clouds* privadas e públicas são flexíveis, escaláveis e de custo relativamente baixo (STAIMER, 2016). Todavia, cada aplicação tem os seus contras e prós.

4.1.3 *Cloud* híbrida

Para fortalecer os benefícios de ambos modelos, surge o conceito de *Cloud* Híbrida, do inglês *Hybrid Cloud*. Uma infraestrutura de *cloud* híbrida combina o conceito de *cloud* privada, pública e comunitária, aperfeiçoando a escalabilidade sob demanda. Um dos recursos deste modelo permite reduzir a carga de uma *cloud* privada em um determinado momento de sobrecarga, ou seja, partilha temporariamente os recursos de uma *cloud* pública a fins de garantir o desempenho da *cloud* privada (AMARANTE, 2013).

4.1.4 *Cloud* comunitária

A infraestrutura de uma *Cloud* Comunitária, do inglês *Community Cloud* é exclusiva e compartilhada por uma comunidade que partilha interesses similares (requisitos de segurança, políticas, considerações de conformidade, entre outros interesses). Pode ser de propriedade, gerenciados e operados por uma ou mais organizações, terceiros, ou ainda a combinação de todos (NIST, 2013, tradução nossa).

4.2 MODELOS DE SERVIÇO NA *CLOUD COMPUTING*

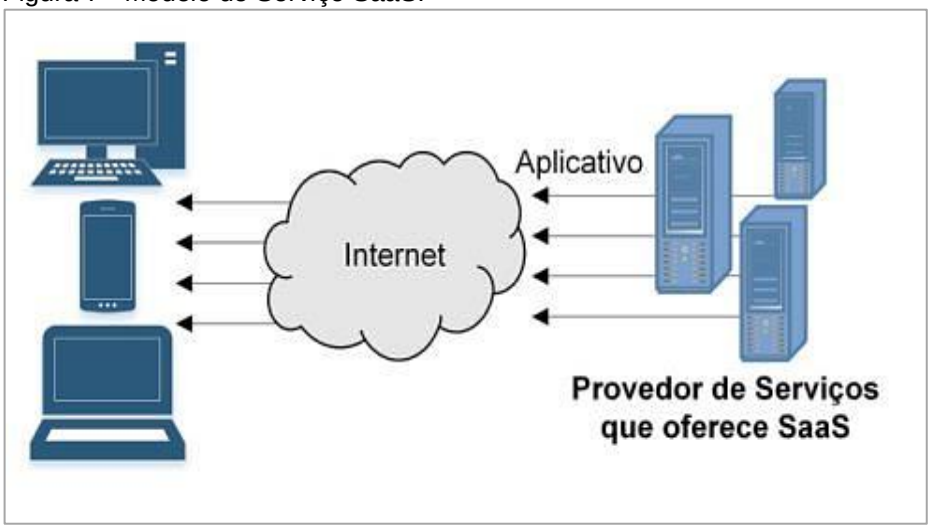
Os ambientes em *Cloud Computing* encontram-se constituídos por diversos modelos de implantação de serviços que são responsáveis por definir o padrão de arquitetura para a *cloud computing* (MICHAEL et al, 2009).

As atuais literaturas classificam os modelos de implantação de serviço em *Software-as-a-Service* (*Software* como Serviço - SaaS), *Infrastructure-as-a-Service* (Infraestrutura como Serviço - IaaS), *Database-as-a-Service* (Banco de Dados como Serviço - DaaS) e *Plataform-as-a-Service* (Plataforma como Serviço - PaaS) e estão classificados de acordo aos recursos fornecidos pelo usuário e de como serão empregados (PEIXOTO, 2012; AMARANTE, 2013).

4.2.1 *Software* como serviço

O modelo de *Software* como Serviço (SaaS) é fundamental para o correto funcionamento da *Cloud Computing* uma vez que constitui a camada estrutural, ou seja, toda arquitetura física (servidores, *data centers*, fontes de energia e climatização). Tal estrutura permite garantir que os serviços e aplicações respondam de forma rápida (ADDED, 2014). A figura 7 representa um modelo de serviço SaaS, onde, o provedor de serviços fornece um aplicativo ou parte de um *software* para várias máquinas (PEREIRA et al, 2016).

Figura 7 - Modelo de Serviço SaaS.



Fonte: Pereira et al (2016).

Neste tipo de modelo os usuários acessam os serviços e aplicações por intermédio de navegadores a partir de endereços URLs conhecidos, mas sem saberem da sua localização física. As ferramentas de produtividade online da *Microsoft* (*onedrive*, *word*, *excel*, entre outras) são exemplos de um modelo de serviço SaaS.

4.2.2 Infraestrutura como serviço

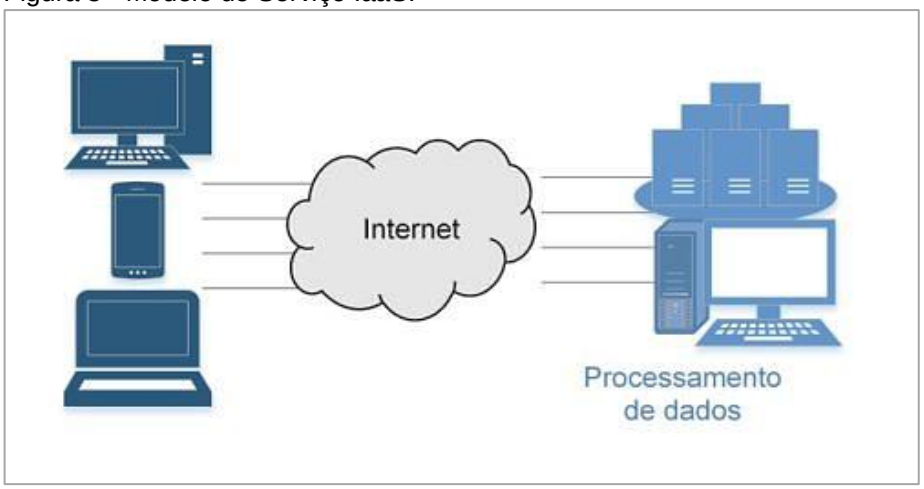
No modelo de Infraestrutura como Serviço (IaaS) os usuários recebem de seus provedores um conjunto de recursos computacionais (processamento armazenamento e redes). O ambiente permite que sejam instalados todos tipos de

softwares, aplicativos e sistemas operacionais. Embora a infraestrutura física esteja oculta para os usuários, eles podem controlar e efetuar alterações nos sistemas operacionais, espaço de armazenamento e aplicativos. A *AmazonWeb Services* (AWS), *Google Computer Engine* e o *Microsoft Azure* são exemplos desse tipo de serviço (OPUS *SOFTWARE*, 2015).

Sousa Neto (2011) explica que o modelo retirou uma preocupação constante das organizações, a de gerenciar *softwares* e licenças nos vários computadores da rede. No ambiente *cloud* deixa de existir esta preocupação, uma vez que não se faz mais necessário obter uma licença para cada computador, e sim, apenas a do servidor.

Na figura 8 é possível observar o conjunto de recursos computacionais fornecidos pelos provedores aos seus usuários.

Figura 8 - Modelo de Serviço IaaS.



Fonte: Pereira et al (2016).

4.2.3 *Database* como serviço

Banco de Dados como Serviço é um modelo de distribuição de informação em que os arquivos de dados como, textos, imagens, sons e vídeos, são disponibilizados aos clientes por meio de uma rede, à Internet. Um provedor de DaaS oferece ótimas soluções de custo-benefício aos seus clientes (ROUSE, 2012, tradução nossa):

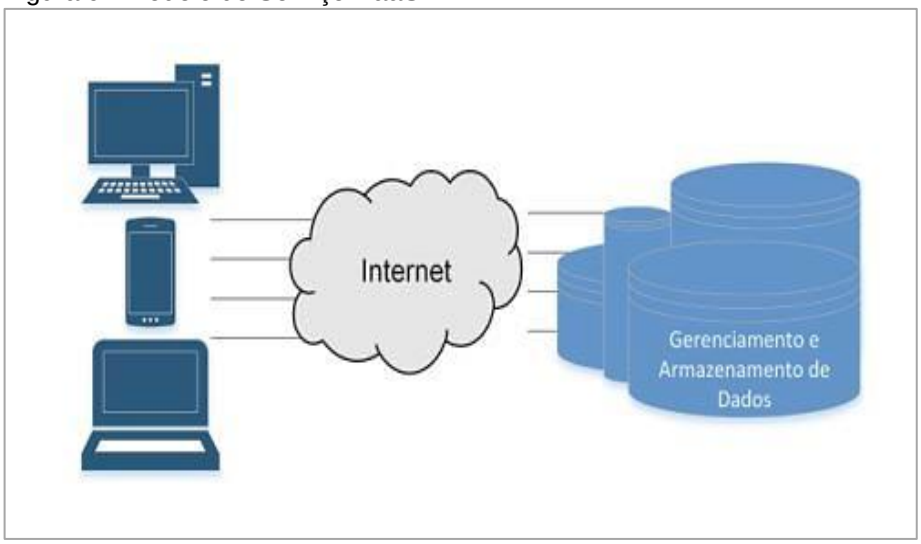
a) possibilidade de mover os dados descomplicadamente de uma plataforma para outra;
b) simplicidade de administração;

c) acessibilidade global;

d) preservação de dados de integridade.

É importante frisar que neste modelo a contratação de bancos adicionais elevam o preço final do serviço em razão da quantidade de dados ser proporcional ao aumento das atividades de gestão, segurança, integração, desempenho e disponibilidade (figura 9) (SEIBOLD; KEMPER, 2012, tradução nossa).

Figura 9 - Modelo de Serviço DaaS.



Fonte: Pereira et al (2016).

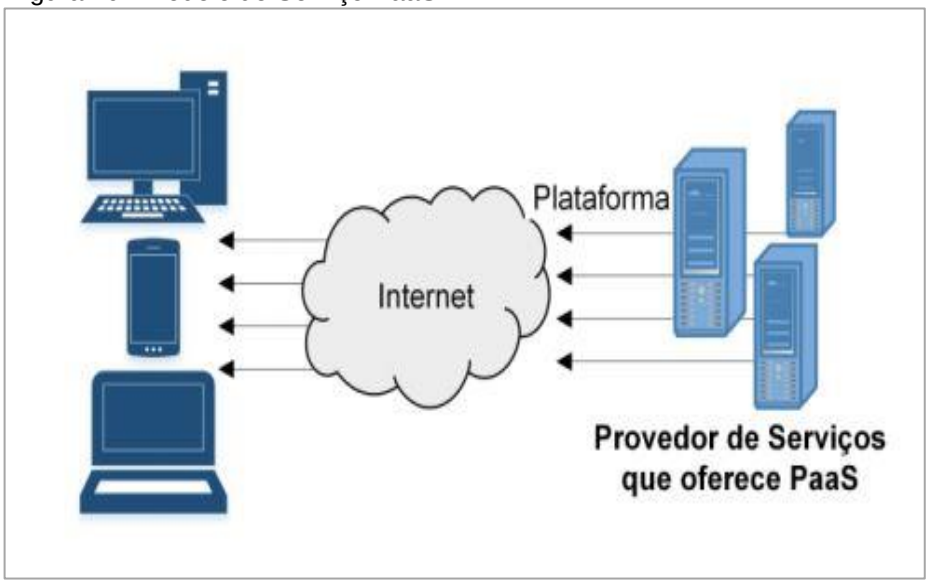
4.2.4 Plataforma como serviço

A Plataforma como Serviço é um dos grandes atrativos da *cloud computing* que se ergueu com o passar dos anos, ajudando a simplificar o desenvolvimento e implantação de serviços e aplicativos. O que caracteriza este ambiente é a combinação de diferentes componentes e serviços para criar um ambiente de aplicação (EARLS, 2016, tradução nossa).

No modelo PaaS, o provedor fornece as ferramentas de *hardware* e *software* de acordo a necessidade do cliente. Ao adquirir este modelo de implantação, os usuários dispensam e necessidade de instalar todo *hardware* e *software* em sua residência, ou em locais de trabalho para o desenvolvimento ou execução de suas aplicações. O modelo PaaS garante flexibilidade, facilidade de manutenção, assim como, a redução para comercialização de novos projetos (ROUSE, 2016, tradução nossa).

Na figura 10 é possível observar um modelo PaaS, onde o provedor de serviços efetua a comunicação com os clientes e autoriza o acesso a sua plataforma computacional que é executada a partir de um sistema em nuvens (PEREIRA et al, 2016).

Figura 10 - Modelo de Serviço PaaS.



Fonte: Pereira et al (2016).

4.3 BENEFÍCIOS DA *CLOUD COMPUTING*

A *cloud computing* não se limita em apenas oferecer recursos de tecnologia, é o que diz o Diretor de Tecnologia da Informação, do inglês *Chief Information Officer* (CIO) do governo dos Estados Unidos de 2009 a 2011. Segundo Kundra (2011, tradução nossa), a *cloud computing* oferece mais benefícios entre os quais destaca a inovação, a agilidade, e a eficiência. Para reforçar esta síntese, a tabela 2 faz a comparação dos benefícios que se destacam em ambientes de computação em *cloud* dos ambientes atuais.

Tabela 2 - Benefícios da *cloud computing*: eficiência, agilidade, inovação.

EFICIÊNCIA	
BENEFÍCIOS DA *CLOUD*	AMBIENTE ATUAL
• Melhor aproveitamento de ativos (utilização do servidor > 60-70%) • Sistema consolidado acelerado, e maior demanda de serviços • Melhor produtividade no desenvolvimento e gerenciamento de aplicativos	• Menor aproveitamento dos ativos (utilização do servidor < 30%) • Sistemas fragmentados e duplicados • Maior dificuldade para gerenciar sistemas
AGILIDADE	
BENEFÍCIOS DA *CLOUD*	AMBIENTE ATUAL
• Compra de *software* como serviço (apenas o acesso da aplicação necessária) • Diminuição de custos • Mais sensível às necessidades dos clientes	• Mais tempo para expansão de centro de dados e serviços • Mais tempo para aumentar a capacidade de serviços
INOVAÇÃO	
BENEFÍCIOS DA *CLOUD*	AMBIENTE ATUAL
• Mudança de foco na gestão de serviços • Inovação no setor privado • Incentiva a cultura empresarial • Maior integração com as tecnologias emergentes. Ex: *smartphones*, *tablets*, entre outros	• Sobrecarregado pelo gerenciamento de ativos • Menos incentivo do setor privado em relação a tecnologia • Central de risco adverso

Fonte: Adaptado de *Kundra* (2011, tradução nossa).

Ainda de acordo com o documento oficial da casa branca, o governo dos Estados Unidos gasta cerca de 80 bilhões de dólares para investimentos no setor de TI, dos quais, 20 bilhões de dólares são investidos na *cloud computing* (KUNDRA, 2011, tradução nossa).

O estudo conduzido pela *OPUS Software* (2015), ressalta que a *cloud computing* possibilitou que todas empresas, independentemente do seu porte e infraestrutura, tenham acesso aos mesmos recursos tecnológicos que só empresas como bancos, instituições governamentais, entre outras, tinham.

4.3.1 Boas razões para as empresas migrarem para a *cloud computing*

Em tempos de crise e com um cenário econômico instável, otimizar a infraestrutura de TI tornou-se uma prioridade para o corte de gastos e até mesmo, em último caso, para sobreviver. A *cloud computing* geralmente causa uma queda nos custos de TI, porque os aplicativos são hospedados pelos fornecedores e provedores conforme demanda, e não por meio de instalações físicas ou por licenças (TURBAN; VOLONINO, 2013).

Por esta razão, a *OPUS SOFTWARE* lista cinco bons motivos para adotar a *cloud computing*:

a) **custo**: a computação em *cloud* adota um modelo dinâmico de alocação e liberação de recursos, este modelo é conhecido pelo termo, pagamento pelo uso, do inglês *pay per use*. O custo de uma infraestrutura local se comparando com o custo na *cloud*, na maioria das vezes acaba por ser mais caro, dado que ocorre uma maior aquisição de máquinas, servidores, firewalls, entre outros.

b) **agilidade**: por mais que os prestadores de serviços convencionais apliquem melhorias na sua logística de despacho e entrega de novas máquinas, ou qualquer outro recurso, na *cloud computing* o processo de alocação (ou diminuição) de novos recursos demora apenas alguns minutos. Seja em soluções de mobilidade ou segurança;

c) **flexibilidade**: infraestruturas de TI tendem a realizar diversas mudanças, seja em termos de espaço físico (necessidade de aumentar o espaço, etc.) ou de serviços (equipamentos mais potentes e atualizados, periféricos, etc.). Ao adotar a tecnologia em *cloud*, estas necessidades passam a ser realizadas instantaneamente;

d) **alta disponibilidade**: adotar a *cloud computing* é mais acessível e garante a alta disponibilidade. Já que para que um ambiente convencional ofereça os mesmos recursos, é necessária uma duplicação, criando um ambiente reserva que passa ser acionado em caso de falha do principal. Esta duplicação implica em desperdícios, gera despesas de depreciação, ocupando espaço, requerendo

> segurança e supervisão, ou seja, há geração de custos mesmo sem a infraestrutura estar no ar (*OPUS SOFTWARE*, 2015).

Ao adotar a *cloud computing* como tecnologia, avalia-se uma redução de custos de TI de até 80%, é o que diz Armbrust et al. (2009, tradução nossa).

4.4 PRESTADORES DE SERVIÇOS PARA À PROTEÇÂO DE ATAQUES DoS

A rede mundial de computadores, popularmente conhecida por Internet, é a responsável pela comunicação de centenas de milhares de conexões existentes nos mais diferentes tipos de dispositivos, mas se por um lado o seu surgimento trouxe diversas vantagens, do outro lado, trouxe também algumas preocupações, ou seja, esta grande estrutura também está vulnerável a diversas ameaças. As mais preocupantes são aquelas que violam os princípios básicos da segurança da informação: integridade, confidencialidade e disponibilidade, sendo que esta pesquisa está centrada especialmente em garantir a disponibilidade (PEREIRA; DANTAS; MEDEIROS, 2012).

Em um mercado competitivo, as organizações precisam avaliar ferramentas e serviços que ofereçam soluções de segurança, sejam estas locais ou em *cloud*. Devem avaliar também quais soluções melhor atendem os requisitos da sua rede considerando as possíveis ameaças que estão expostas, sejam elas internas ou externas. Esta pesquisa terá foco em um serviço de monitoramento e mitigação de ataques de negação de serviço, à *Maxihost*.

4.4.1 *MaxiHost*

Fundada em 2001 e com sede em São Paulo e *Nova York*, a *Maxihost* começou por oferecer serviços de hospedagem de *websites* em *data centers* fora do país, hoje, a empresa conta com mais de cinco *data centers* no Brasil e não para de crescer. Suas soluções partem de serviços gerenciados (backup como serviço, monitoramento, proteção de ataques DoS) e mercado (jogos, *e-commerce*) (MAXIHOST, 2016b).

Atualmente possuímos uma capacidade total de mitigação nacional de até 20 Gbps, e 100 Gbps internacional (LIMA, 2016).

4.4.1.1 Proteção DoS/DDoS

Um dos segredos do sucesso da tecnologia de proteção da *Maxihost* está no uso dos equipamentos da *NsFocus*, uma provedora de soluções e serviços de segurança de rede com mais de uma década no mercado de segurança (LIMA, 2016; NSFOCUS, 2016, tradução nossa).

Ao combinarem o sistema de defesa de ataques ADS da *NsFocus*, do inglês *Anti-DoS System (ADS),* a sua tecnologia de proteção, à *Maxihost* passou a oferecer mais flexibilidade e facilidade na utilização dos seus serviços (LIMA, 2016).

O sistema de proteção ADS possui uma arquitetura escalável, o que na prática garante uma performance otimizada. O Sistema está composto por três componentes (NSFOCUS, 2016, tradução nossa):

a) ***Network Traffic Analyzer* (NTA):** tem a função de detectar ameaças e identificar o tráfego malicioso;
b) ***Anti-DoS System* (ADS):** permiti mitigar todo o tráfego malicioso, ou seja, o tráfego indesejado;
c) ***Anti-DoS System Manager* (ADS-M):** é uma ferramenta de gestão centralizada que permite o controle e suporte dos usuários, e os módulos NTA e ADS.

De acordo à *Maxihost* (2016c), os seus mecanismos de proteção para ataques DoS são pioneiros no Brasil. A empresa garante que detecta e bloqueia ataques sem prejudicar o *cloud server* ou servidor dedicado.

Quando a tecnologia de proteção é instalada à *Maxihost* passa a fazer toda análise do tráfego, segregando o tráfego malicioso do tráfego legítimo de forma automática. A empresa oferece as seguintes soluções para proteção e mitigação de ataques (MAXIHOST, 2016c):

a) **proteção para sites**: basta apontar os DNS do seu site para a *Maxihost*, e através de nosso *proxy* reverso, redicionaremos todas as requisições HTTP/SSL para seu servidor original. O IP visível para Internet e consequentemente para o hacker será nosso. Os pacotes maliciosos serão descartados e todo tráfego limpo direcionado ao seu site;

b) **proteção para servidores**: aplicações hospedadas dentro de nossos c*loud servers* e servidores dedicados e que estejam a precisar de proteção contra estas ameaças, serão instalados em uma rede exclusiva e preparada;
c) **proteção para redes**: integre seu provedor de acesso à Internet (ISP) com a rede da *Maxihost* e esteja protegido contra possíveis ataques.

4.4.1.2 Monitoramento

O monitoramento de uma rede baseia-se na análise de informações e dados a ser interpretados e avaliados para o seu correto funcionamento (MOTA FILHO, 2013).

O uso de ferramentas de monitoramento possibilita à análise de possíveis ameaças (internas e externas) que representem riscos para os servidores, e a configuração de eventos (*e-mail*, celular, entre outros) que possam dar a conhecer aos administradores e assim tomar as devidas medidas (CÉLESTIN, 2013).

Para contornar estas situações é extremamente importante que as organizações adotem soluções avançadas de monitoramento. Ao implementarem uma estratégia de monitoramento, estas não se limitam em apenas saber se seus sites ou aplicações estão online, mas passam também a ter um controle da qualidade de navegação (MAXIHOST, 2016a).

Ao combinar o sistema *Network Traffic Analyzer (NTA)* junto com algumas ferramentas como o *Nagios*, *Ubersmith*, *Cacti*, *The Dude*, entre outras utilizadas (divulgação não autorizada), além de boots integrados aos sistemas de chat interno, a empresa garante uma solução estratégica de monitoramento (LIMA, 2016).

4.4.1.3 Detecção e separação de tráfego

Para detectar e separar tráfego malicioso de uma rede, os equipamentos efetuam uma análise e inspeção severa a partir de um motor multiestágio do sistema *Anti-DoS System (ADS)*. A ação garante que todos os protocolos sejam submetidos a uma série de algoritmos de análise e inspeção (NSFOCUS, 2016, tradução nossa).

Outros mecanismos são também utilizados para garantir a detecção do tráfego malicioso (NSFOCUS, 2016, tradução nossa):

a) verificações a partir de comandos (RFC);
b) análise de protocolos;
c) lista de controle de acesso;
d) reputação do IP (*blacklists*, entre outros);
e) *anti-spoofing*;
f) análise algorítmica nas camadas 3 e 4 do modelo OSI.

Além da análise e comportamento dos usuários, aplicações, controle e limitações na taxa de conexão. Para garantir uma proteção ainda mais segura, o motor multiestágio do sistema ADS recebe constantes atualizações (NSFOCUS, 2016, tradução nossa).

4.4.1.4 Mitigação

Como já mencionado anteriormente, o componente responsável por detectar qualquer tráfego malicioso na rede é o *Network Traffic Analyzer* (NTA), entretanto, quando detectado é o componente *Anti-DoS System* (ADS) que fica a cargo de mitigar o ataque (NSFOCUS, 2016, tradução nossa).

Segundo a NsFocus (2016, tradução nossa) o processo de mitigação consiste exclusivamente em garantir e entregar apenas o tráfego legítimo ao destino, sendo que, todo tráfego malicioso é removido pela central de mitigação (figura 11).

Para complementar o sistema de defesa, existe ainda uma Interface de Programação de Aplicação (*Application Programming Interface* - API) de serviços WEB pós-incidentes, que visam auxiliar na análise forense (NSFOCUS, 2016, tradução nossa).

Figura 11 - Mitigação do tráfego malicioso.

Fonte: *NsFocus* (2016).

Feita a análise da figura, é importante frisar que durante o ataque o sistema gera relatórios em tempo real, são informações valiosas como o tipo de ataque, a fonte e o destino (ISP) do ataque, os protocolos que estão a ser utilizados, a quantidade de pacotes enviados e recebidos, entre outras várias informações que auxiliam os usuários do sistema (NSFOCUS, 2016, tradução nossa).

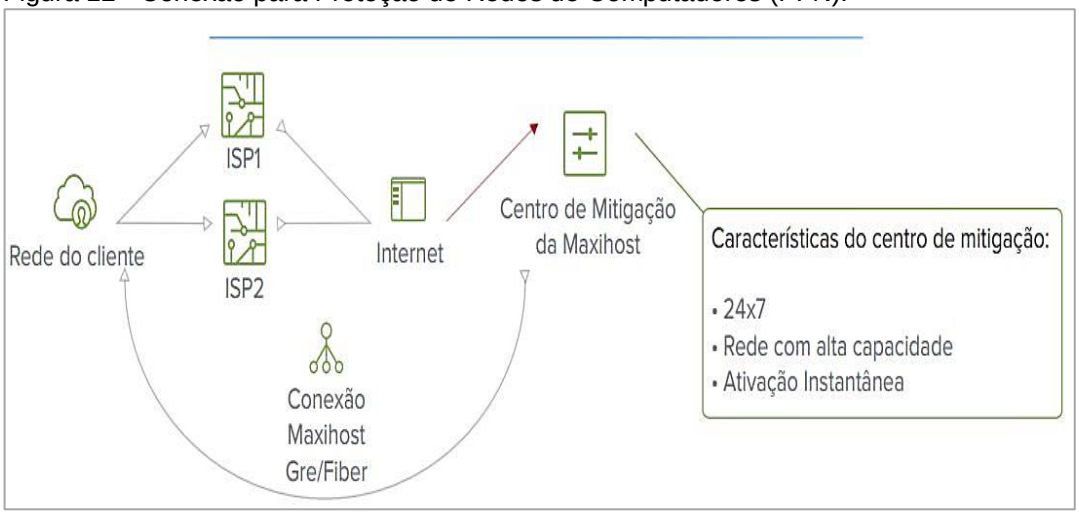
A prevenção e mitigação contra-ataques DoS que à *Maxihost* oferece, está dividida em dois tipos principais (MAXIHOST, 2016d):

1) a **Proteção para Redes de Computadores** (*Protection for Networks* - PFN);
2) a **Proteção para Serviços** (*Protection for Services* - PFS).

Para se conectar à *Maxihost* utilizando a PFN e garantir que o seu *cloud server* não seja prejudicado por ataques DoS, é necessário (figura 12):

a) conectar-se fisicamente (fibra/cobre) ou virtualmente (tunelamento de Encapsulamento de Roteamento Genérico, *Generic Routing Encapsulation* - GRE);
b) configurar à rede para anunciar à "*Maxihost*" como um dos provedores de Internet;
c) decidir o quanto de tráfego pretende rotear através da *Maxihost*.

Figura 12 - Conexão para Proteção de Redes de Computadores (PFN).

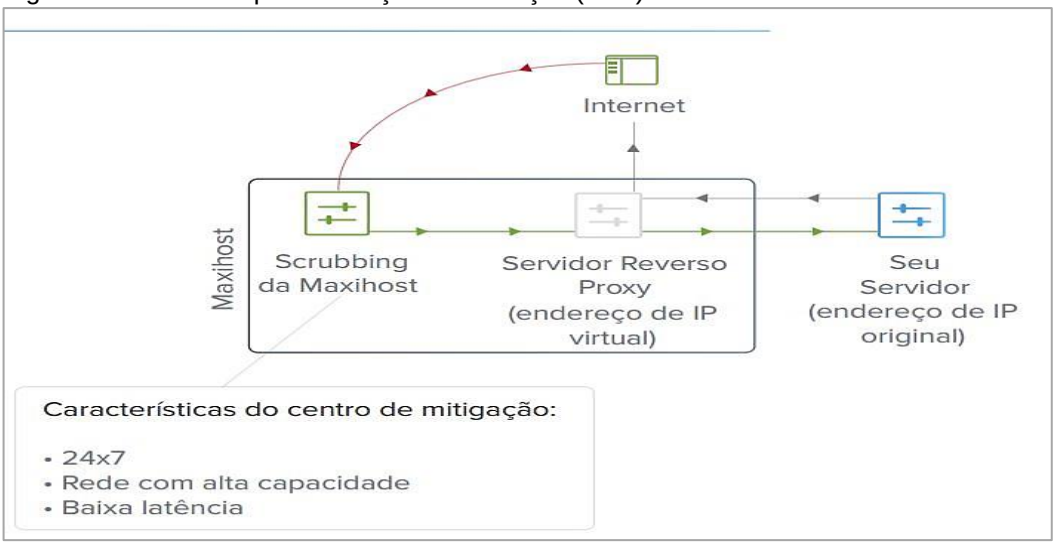


Fonte: *Maxihost* (2016d).

Feita a configuração, todo tráfego roteado passa a ser filtrado para garantir que apenas o tráfego legítimo atinja à rede (MAXIHOST, 2016d).

Já para configurar a Proteção de Serviços (PFS), basta apontar o DNS para um endereço de IP fornecido pela *Maxihost* (figura 13) (MAXIHOST, 2016d).

Figura 13 - Conexão para Proteção de Serviços (PFS).



Fonte: *Maxihost (*2016d).

Para complementar os esclarecimentos acima retratados, vide anexo C para visualizar mais informações de quais camadas do modelo OSI cada tipo de proteção atua, tal como outras características técnicas, e benefícios da sua utilização.

4.4.1.5 Desempenho, qualidade e valores

O desempenho de uma rede é medido por diversos fatores, sendo um dos mais importantes, a segurança. Ao adotar um sistema avançado de proteção baseado na *cloud computing* alivia algumas preocupações pertinentes a este fator.

A chave para manter o equilíbrio QoS de uma rede, é uma boa gestão de tráfego (NOLLE, 2009, tradução nossa).

As informações acerca dos planos e cláusulas do Acordo de Nível de Serviço, do inglês *Service Level Agreement* (SLA), podem ser consultas no anexo D.

5 TRABALHOS CORRELATOS

No decorrer desta pesquisa, estudaram-se outros trabalhos da comunidade acadêmica e científica semelhantes ao que esta pesquisa retrata. A seguir, é feito um resumo destes, abordando temáticas voltadas ao monitoramento, desempenho e proteção das redes de computadores.

5.1 *BENCHMARKS FOR DDoS DEFENSE EVALUATION*

Foi apresentado por *Mirkovic* et al. (2006), pela *University of Delaware*, publicado na *Military Communications Conference* no ano de 2006, e adicionado à biblioteca digital IEEE *Xplore* no ano de 2007, como artigo no âmbito acadêmico e cientifíco.

O estudo teve como finalidade a criação de uma metodologia que servisse de base para avaliação e comparação independente de ataques de negação de serviço (DoS). A metodologia consistiu em definir os elementos e métricas necessárias para aplicação de cenários de ataque DoS, assim como os serviços e recursos necesários.

O trabalho foi de acordo e serviu de métrica para o desenvolvimento do estudo de caso desta pesquisa, quando se levou em consideração os princípios fundamentais para a elaboração do cenário de aplicação e testes.

5.2 MÉTODO DE MITIGAÇÃO CONTRA ATAQUES DE NEGAÇÃO DE SERVIÇO DISTRIBUÍDOS UTILIZANDO SISTEMAS MULTIAGENTES

Desenvolvido por João Paulo Aragão Pereira, no curso de Engenharia de Computação, pela Escola Politécnica, Unidade de São Paulo, no ano de 2014, como trabalho de Conclusão de Curso, para obtenção do grau de Mestre, sob orientação do Prof. Dr. Marcos Antônio Simplício Júnior.

Pereira (2014) explicou que a qualidade de serviço (QoS) oferecida pelos Provedores de Internet, do inglês *Internet Service Provider* (ISPs) depende diretamente da quantidade de recursos disponíveis no momento. Entretanto, essa qualidade tem sido afetada por ataques que consomem todos esses recursos, os mais comuns, ataques de Negação de Serviço Distribuídos. (DDoS). Com isso, João

Pereira desenvolveu uma ferramenta capaz de monitorar e detectar algum tráfego análogo. Concluiu seu objetivo ao criar uma ferramenta local capaz de monitorar, detectar e mitigar ataques de Negação de Serviço. Entretanto, mitigar ataques de Negação de Serviço é uma tarefa desafiadora devido à natureza distribuída desses ataques, com isso, o autor propôs como trabalho futuro uma solução que fosse capaz de apenas bloquear o tráfego malicioso, não correndo o risco de bloquear o tráfego legítimo da rede.

Este trabalho foi de encontro com o objetivo desta pesquisa, proteger os ativos das organizações e propor uma solução para mitigar ataques DoS. Entretanto, a ferramenta utilizada nesta pesquisa apresentou uma diferença mais significativa, sendo capaz de diferenciar o tráfego legítimo e malicioso, ocasionando num bloqueio maior do tráfego malicioso. Há que se mencionar também, que Pereira (2014) abordou sobre uma solução de mitigação local, enquanto a presente pesquisa aborda uma solução baseada na *cloud computing*.

5.3 MITIGAÇÃO DE ATAQUES DE NEGAÇÃO DE SERVIÇO EM *RESTS* AUTENTICÁVEIS NA NUVEM

O trabalho foi desenvolvido por Régio Antonio Michelin, no curso de Ciência da Computação, pela Pontifícia Universidade Católica do Rio Grande do Sul, no ano de 2015, para obtenção do grau de Mestre, sob orientação do Prof. Dr. Avelino F. Zorzo.

Michelin (2015), retratou sobre a crescente exposição de ameaças ao qual os sistemas de informação se encontram. Destacou ameaças de diferentes topologias e o comportamento que adotam. O autor reforça a atenção especial que os ataques de negação de serviço devem ter, especialmente quando o alvo são os ambientes em nuvem, pois são várias as razões que servem de incentivo para esta ameaça. O seu estudo teve como finalidade fornecer uma solução que atua em nível de aplicação, traçando um perfil dos clientes que fazem uso do mecanismo de autenticação REST API em ambientes *cloud computing,* evitando assim que sejam sobrecarregados com operações desnecessárias.

A pesquisa desenvolvida adota uma ótica oposta, a de utilizar o ambiente em nuvem como solução. No entanto, destaca-se que o ambiente utilizado adota uma infraestrutura diferente e adequada para lidar com ataques DoS. Na ausência deste

modelo, ambientes em nuvem tornam-se um potencial vetor de ataques DoS. Desta forma, recomenda-se que se agregue às técnicas já existentes de segurança, soluções que protejam os ambientes desta ameaça.

5.4 ANÁLISE DE TRÁFEGO DE DADOS EM REDES LOCAIS: ESTUDO DE CASO NA UNESC

O trabalho foi apresentado por Eduardo de Souza Zardin, no curso de Ciência da Computação, pela Universidade do Extremo Sul Catarinense, no ano de 2016, como Trabalho de Conclusão de Curso, para obtenção do grau de Bacharel, sob orientação do Prof. MSc. Rogério Casagrande.

Zardin (2016) fez o monitoramento de dados de tráfego em uma rede local tendo como finalidade buscar evidências de uso inadequado de recursos nos laboratórios de informática da Universidade. Para alcançar seu objetivo, seu estudo analisou o funcionamento de uma rede de computadores e a comunicação entre os dispositivos, explicando alguns protocolos de comunicação da arquitetura TCP/IP. Seguindo de um estudo detalhado de cinco ferramentas de monitoramento (*sniffers*), e um método estatístico para analisar, coletar e documentar os dados obtidos. Ao final alcançou seu objetivo ao fazer uma análise na rede onde foi possível identificar possíveis problemas que pudessem afetar o desempenho da rede.

Este trabalho foi de encontro há um dos objetivos desta pesquisa, o monitoramento de redes. Entretanto, esta pesquisa apresentou algumas diferenças significativas, como o método de monitoramento, e no estudo de caso proposto.

5.5 *COMPUTER SECURITY INCIDENT HANDLING GUIDE: RECOMMENDATIONS OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY*

Este trabalho foi apresentado por *Paul Cichonski*, *Tom Millar*, *Tim Grance* e *Karen Scarfone*, publicado pelo *National Institute of Standards and Technology* (NIST), *Department of Commerce*, *United States*, no ano de 2012, como trabalho científico, sob supervisão do Diretor e Subsecretário Patrick D. Gallagher.

O estudo teve como objetivo categorizar e orientar as organizações a maneira correta de como reportar incidentes de segurança. Cichonski et al. (2012, tradução nossa) fizeram uma avaliação do quão importante se tornou os programas

de resposta a incidentes de segurança. Reportar incidentes é uma tarefa complexa e seu correto funcionamento requer planejamento e recursos substanciais. Ao final, os autores concluíram seus objetivos ao criarem um guia que auxilia as organizações a se prepararem bem como a maneira correta de reportarem incidentes de segurança.

6 ESTUDO DE UM CASO DE ATAQUE DE NEGAÇÃO DE SERVIÇO, UTILIZANDO UMA CONTRAMEDIDA DE MITIGAÇÃO BASEADA NA *CLOUD COMPUTING*

Os serviços da *cloud* pública ou redes de computadores não estão imunes as várias ameaças de segurança existentes, e uma boa parte destas ameaças envolvem ataques de negação de serviço. Cibercriminosos não se limitam apenas ao roubo de dados, eles podem ocasionar falhas nas aplicações com solicitações de tráfego malicioso. A ferramenta mais comum contra este tráfego indesejado tem sido o *firewall* tradicional. No entanto, o gerenciamento de um *firewall* tende a ser problemático e demorado, especialmente para ataques DDoS, o volume de tráfego gerado é sempre muito alto, é o que explica *Stephen Bigelow*, editor de tecnologia sênior com mais de 20 anos de experiência e com certificação *CompTIA* em segurança de redes de computadores e servidores (BIGELOW, 2016, tradução nossa).

Por sua vez, Pereira (2014) explica que o que classifica a boa ou má eficiência de um sistema de defesa, é a sua capacidade de assegurar que as propriedades básicas de segurança disponibilidade, integridade e confidencialidade não sejam violadas.

Esta pesquisa teve como finalidade avaliar o comportamento de um ataque DoS *SYN Flood*, e da contramedida de mitigação fornecida pela *Maxihost*[18]. Um ataque DoS, é caracterizado principalmente por violar as propriedades básicas da segurança, especialmente a propriedade da disponibilidade.

O presente trabalho foi realizado em um dos polos da Universidade Aberta do Brasil (UAB), localizado em Criciúma/SC, e pela empresa *Maxihost* (via acesso remoto), localizada na Vila Mariana/SP. Foi solicitado por escrito um ofício ao Polo UAB de Criciúma, a fim de obter a devida autorização para realização do estudo de caso (apêndice A). Seguidamente foi recebida, do coordenador do polo, a devida resposta (anexo A).

[18] Fundada em 2001, a empresa atua no mercado há mais de quinze anos, e é provedora de soluções de servidores *cloud* e dedicado que mais cresce no Brasil. A *Maxihost* oferece serviços de *cloud computing*, *hosting* dedicado, *colocation* e serviços de gerenciamento (*backup* e *storage*, monitoramento e proteção DoS). A sua tecnologia de proteção contra-ataques DoS e DDoS é exclusica e pioneira no Braisl. A empresa possui mais de cinco datacenters incluindo um próprio, Tier Três *compliant*, inaugurado em 2015 e com capacidade para 10.000 servidores. Opera nos Estados Unidos (*Nova York*) e Brasil (São Paulo) (MAXIHOST, 2016b).

Para a realização do presente trabalho definiu-se três situações, (1ª) ataque, (2ª) defesa, (3°) vítima. A execução do ataque foi originada a partir de Criciúma, enquanto que a vítima do ataque e a abordagem de defesa encontravam-se na rede da *Maxihost*, SP.

Agora, para elucidação e contextualização deste estudo de caso, dando ênfase às suas etapas, precisamos de entender o seguinte:

a) **a primeira situação é representada por um cenário de ataque:** onde um indivíduo realiza um ataque DoS, e tenta sobrecarregar à rede com mais requisições de acesso do que àquelas que um servidor suportaria;
b) **a segunda situação é representada por um cenário de vítima:** onde um usuário legítimo desta rede, que realiza as suas atividades rotineiras, (acesso a sites acadêmicos e a sites corporativos, entre outras atividades) deixa de obter respostas do servidor por ser vítima de um crime digital;
c) **a terceira e última situação é representada por um cenário de defesa:** onde apresenta-se a abordagem de defesa e mitigação contra-ataques DoS da *Maxihost*.

Importa mencionar que o presente método de proteção não sofreu qualquer interferência do acadêmico, uma vez que o procedimento de defesa é automatizado e, quando necessário, apenas à *Maxihost* tem acesso ao sistema. No entanto, foi disponibilizado ao acadêmico dois painéis de monitoramento do sistema para auxílio e geração de alguns dados estatísticos.

A instalação e configuração das ferramentas, bem como as técnicas aplicadas, serão descritas nas próximas etapas do trabalho.

Uma vez entendido os cenários e esclarecidos alguns pontos, segue-se com os conceitos pertinentes à metodologia científica aplicada neste trabalho.

6.1 METODOLOGIA

Para materialização deste trabalho de conclusão de curso, procedeu-se a um levantamento bibliográfico específico, focado no tema de defesa, seguido de uma análise e síntese para identificação da matéria pertinente e imprescindível à sua concepção. Parte das obras disponibilizadas são de origem anglófona, e integram artigos científicos e dissertações para títulos de bacharel e mestre, encontrando-se

hospedadas em repositórios científicos como o Repositório Científico de Acesso Aberto de Portugal, os Periódicos CAPES, a Biblioteca Digital *IEEExplore* e Jornais Científicos, entre outros. No decorrer da pesquisa, fez-se necessário deslocar à *Maxihost* para consolidar a parceria e obter informações complementares.

Logo após a identificação de todo material pertinente a pesquisa, deu-se início a elaboração e aplicação do cenário de ocorrência do crime digital.

6.2 DEFINIÇÃO DA EMPRESA DE PROTEÇÃO

Nesta etapa da pesquisa, foi feita a procura da empresa que pudesse fornecer e garantir a proteção contra-ataques DoS. Das empresas pesquisadas, foi à *Maxihost* que abriu as portas e forneceu o apoio necessário para o desenvolvimento deste estudo.

Após definida a empresa, e na sequência da implementação prática, pensou-se em criar-se os cenários (ataque-vítima) em Criciúma, no entanto, seria necessária uma ligação física (fibra/cobre), ou virtual (protocolo de tunelamento - GRE) à rede da *Maxihost.*

Ambas as soluções não foram aplicadas em razão da inviabilidade e por suplantarem os limites financeiros do acadêmico, algo que não se aplica para entidades empresarias e educacionais, em razão da sua estrutura financeira. Para contornar esta insuficiência, criou-se a vítima dentro da própria rede da *Maxihost,* liberando o acesso remoto à mesma. Na prática, esta ação permitiu simular o comportamento de um usuário legítimo da rede.

É importante frisar, que para a realização dos testes e para que nenhuma política de segurança e/ou de direitos autorais fosse infringida, fez-se necessária a redação de outro ofício dirigido à *Maxihos*t, solicitando a devida autorização (apêndice B). Seguindo por escrito a devida resposta autorizando a solicitação feita (anexo B).

6.3 RECURSOS

O cenário da aplicação prática baseou-se em uma avaliação crítica e foi promovido levando em consideração o modelo *Benchmarks for DDoS Defense Evaluation,* publicado por Mirkovic et al (2006, tradução nossa) na biblioteca digital *IEEExplore*.

O artigo do autor define três princípios fundamentais que servem como uma ótima orientação para testes de ataques DoS:

a) serviços e recursos necessários para originar um ataque DoS;
b) serviços e recursos para geração de tráfegos legítimo e malicioso;
c) diferentes topologias de rede.

A abordagem do tipo de ataque baseou-se na utilização de uma ferramenta que pudesse manipular pacotes de dados, gerar o tráfego malicioso, analisar portas e testar regras de *firewalls*.

Para a defesa, adotou-se uma arquitetura de análise e inspeção do tráfego na rede. A solução está embasada na *cloud computing* e é capaz de mitigar ataques sem prejudicar o *cloud server*.

A topologia de serviços e equipamentos utilizados não é comparável a um verdadeiro ataque DoS/DDoS, mas levando em consideração os resultados que foram obtidos, a topologia mostrou ser uma ótima referência. Utilizou-se o *software The Dude,* para detecção dos equipamentos da rede de testes e mapear visualmente a topologia das redes.

No geral, os recursos que foram necessários para desenvolver a pesquisa foram:

a) 3 computadores;
b) 2 servidores *Linux Debian Jessie*;
c) conexão de banda de 20 Mbps de d*ownload/upload*;
d) *software's VirtualBox, The Dude, Hping, MobeXterm, Nagios, Ubersmith, Cacti;*
e) Proteção *Anti-DoS cloud computing;*
f) Painéis de monitoramento ADS-M;
g) outras ferramentas hospedadas no ambiente cuja divulgação não foi permitida.

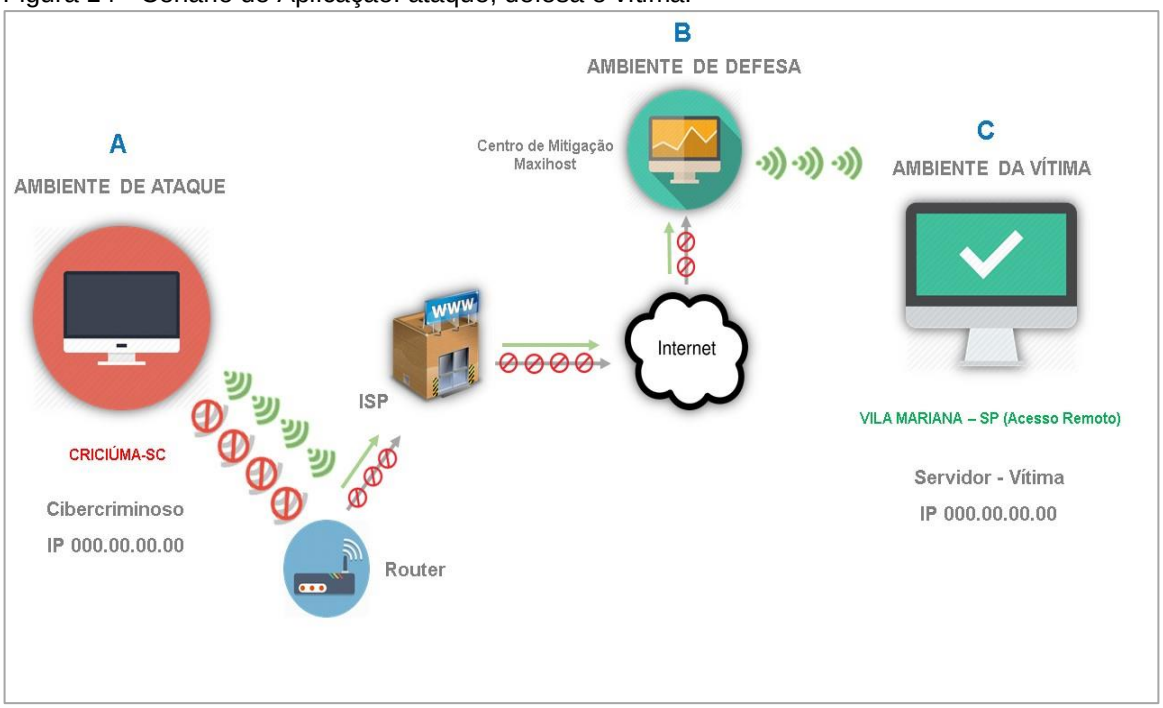
6.4 CENÁRIO DE APLICAÇÃO

Como mencionado anteriormente, considerou-se à ocorrência de um crime digital, onde um indivíduo de má índole utiliza os seus conhecimentos para tirar proveito de uma determinada situação.

É sabido que a execução do crime surge quando o atacante estabelece uma comunicação cliente-servidor pelo protocolo TCP/IP. Entretanto, esta não vem a ser uma conexão normal, pois o criminoso pretende sobrecarregar o servidor com o maior número possível de requisições de acesso até que este pare de dar respostas.

Acompanhe na figura 14 de forma generalizada, o fluxo de tráfego na rede dos ambientes de ataque, defesa e vítima. Torna-se evidente que o ambiente C (vítima) está sobre um ataque DoS.

Figura 14 - Cenário de Aplicação: ataque, defesa e vítima.



Fonte: Do autor (2016).

Ainda de acordo à figura 14, observa-se a existência de dois tipos de tráfego (legítimo e malicioso) que circulam nos ambientes. No entanto, o ambiente da vítima encontra-se protegido contra este tipo de ataque, de tal modo que o tráfego ao passar pelo centro de mitigação, passa de imediato a receber o devido tratamento. O procedimento resulta na saída e entrega apenas do tráfego legítimo, impedindo que o servidor-vítima fique total ou parcialmente fora do ar.

Uma vez esclarecido o cenário de aplicação, torna-se necessário mencionar os recursos que foram utilizados neste estudo de caso:

a) um servidor virtual de ataque com sistema operacional *Linux Debian Jessie*;

b) um servidor de ataque remoto VPS com sistema operacional *Linux Debian Jessie* (acesso remoto);
c) um servidor vítima dedicado com sistema operacional *Windows Server* 2008 R2 (acesso remoto);
d) os *softwares Hing,* versão 3, *VirtualBox,* versão 5, *Mobaxterm;*
e) dois painéis de monitoramento da *Maxihost* integrados com as ferramentas *Nagios*, *Cacti* e *The Dude* (para dados estatísticos, análise e captura de pacotes).

6.4.1 Cenário de ataque

É importante mencionar que os ataques DoS não funcionam a partir de conexões residências, em razão da baixa taxa de *upload*. Uma situação que é comum se levarmos em consideração, que a maioria das operadoras de Internet apenas fornecem 10% de taxa de *upload* da velocidade contratada.

Como no início dos testes desta pesquisa, ainda não se havia obtido a devida autorização para realização dos testes nos laboratórios do Polo UAB de Criciúma, contratou-se um Servidor Virtual Privado (*Virtual Private Server* - VPS)[19] remoto da empresa *Contabo*, situada na Alemanha. O servidor permitiu iniciar os primeiros testes e entender o funcionamento de um ataque DoS.

Para complemento da explicação, acompanha-se na tabela 3 as características deste servidor.

Tabela 3 - Servidor VPS.

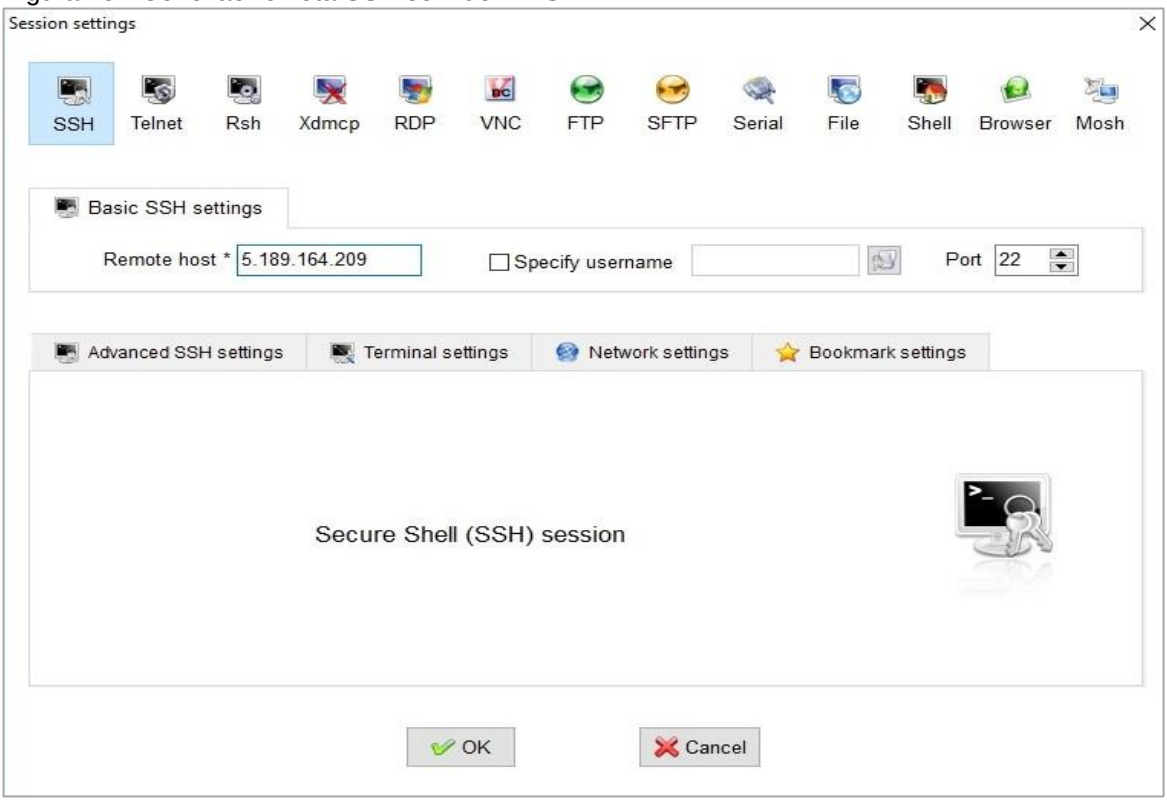
CPU	2 Núcleos
RAM	6 GB
Armazenamento SSD	500 GB
Porta / Largura de Banda	100 Mbit/s port / Tráfego Ilimitado
UpLink	20 Gbit/s
Sistema Operacional	*Linux Debian 8 (Jessie)*
Suporte	3.16.0-4-amd64
Hostname	*root*@servidordeataquetestes
Endereço IP	5.189.164.209

Fonte: Do autor (2016).

[19] permite executar diferentes aplicações e serviços dentro de um único servidor físico. VPS's permitim acesso administrativo (*root*), aos seus cleintes (ROUSE, 2007c, tradução nossa).

A conexão a este servidor VPS foi feita a partir da ferramenta *MobaXterm*. A ferramenta permite realizar conexões remotas a servidores remotos utilizando os protocolos SSH, *Telnet*, Rsh, Xdmcp, RDP, VNC, FTP, SFTP, entre outros tipos de comunicação. A figura 15 ilustra o momento de conexão ao servidor VPS.

Figura 15 - Conexão remota SSH servidor VPS.



Fonte: *MobaXterm* (2016).

Escolhido o tipo de conexão e fornecido o endereço IP, foram solicitadas as credencias de administração para acesso. Uma vez autenticadas as credencias, o *MobaXterm* disponibilizou um terminal *Unix/Linux*, que permitiu estabelecer uma comunicação direta com o VPS.

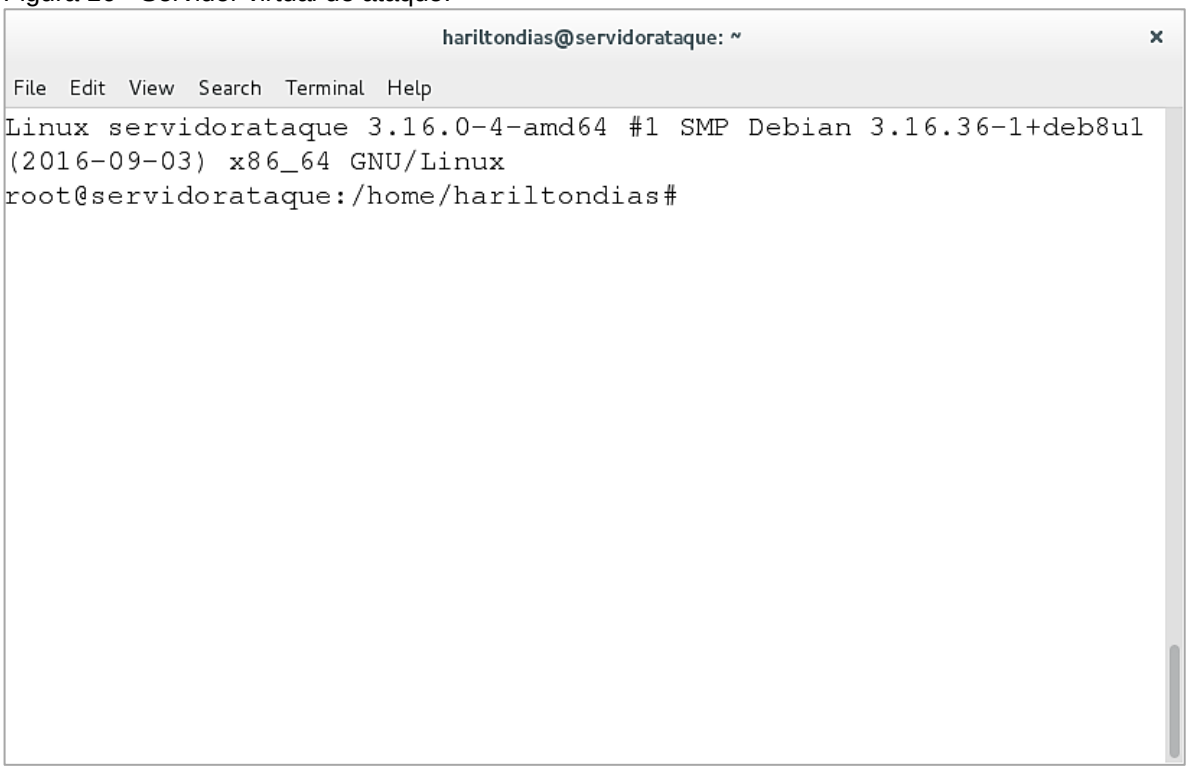
O número de servidores VPS's contratados são proporcionais ao tamanho do ataque que se deseja realizar, ou seja, quanto mais servidores VPS forem contratados, mais tráfego malicioso será gerado. Para compreender o funcionamento de um ataque DoS, precisou-se apenas de um servidor.

No final, com o ambiente de ataque VPS's configurado, foi possível realizar os primeiros testes e posteriormente obter o conhecimento necessário sobre o uso das técnicas necessárias para realizar o ataque.

Após obtida a devida autorização (anexo A) para a realização dos testes no ambiente do Polo UAB, definiu-se os horários matutino e vespertino para realização dos testes e coleta das amostragens. Os horários foram definidos levando em consideração as atividades realizadas no ambiente, evitando desta forma, comprometer a rede no seu período de atividade.

O passo seguinte, foi instalar e configurar um servidor local de ataque com o sistema operacional *Linux Debian Jessie*. A escolha deste sistema foi dada principalmente pela sua estabilidade e desempenho (figura 16).

Figura 16 - Servidor virtual de ataque.



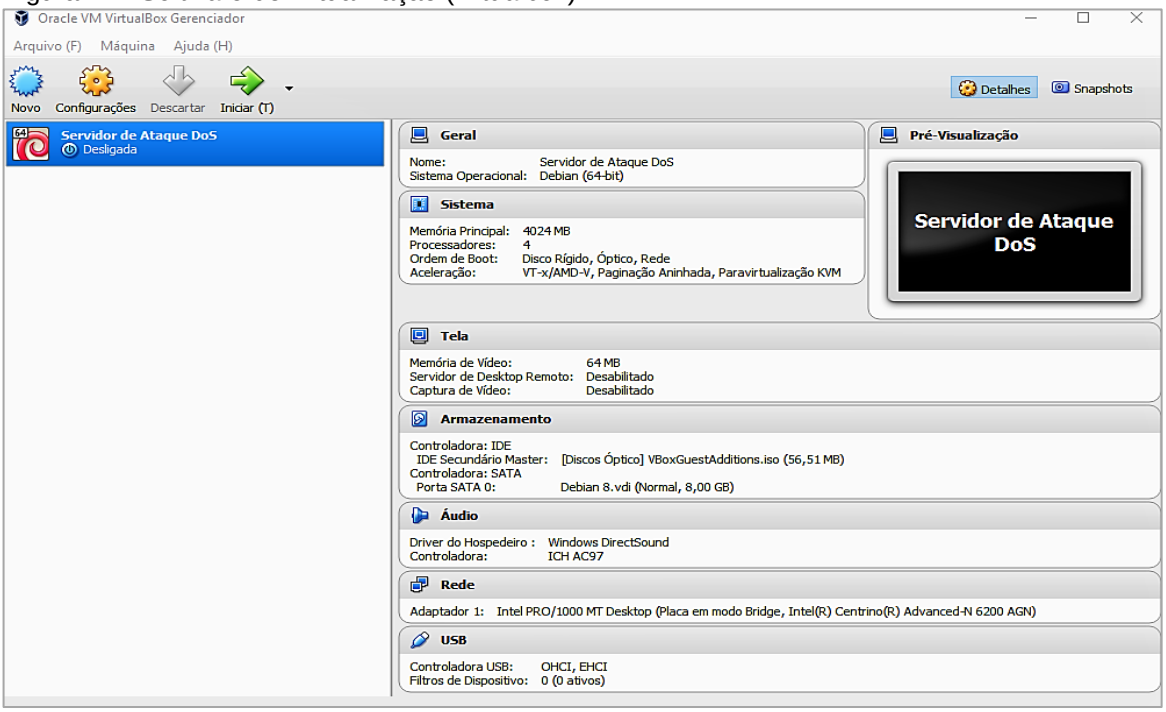
Fonte: Do autor (2016).

Para emular o servidor de ataque foi utilizada a ferramenta da *Oracle Corporation*, o *Virtualbox,* na sua versão 5.1.8. A ferramenta possui um espaço conceituado no mercado quando o assunto é emulação de sistemas operacionais.

Considerando já a existência de ótimos guias de instalação tanto do *VirtualBox,* como do sistema operacional *Linux Debian*, e também com a intenção de não estender em demasia esta pesquisa, fica como referência o guia feito pelo professor Anderson Favaro, da Universidade de Guarulhos (UNG) (FAVARO, 2010).

Sendo assim, a figura 17 demonstra este servidor já devidamente instalado e configurado.

Figura 17 - *Software* de virtualização (*virtualbox*).



Fonte: *Oracle Corporation* (2016).

A ferramenta utilizada para a realização do ataque foi o *Hping*, embora existam outras ferramentas com o mesmo propósito, como é o caso do T50, ou ainda o *Metasploit*. A escolha do *Hping,* embasou-se na pesquisa bibliográfica feita. O uso do *Hping* permite manipular vários valores do cabeçalho TCP/IP, o tamanho dos pacotes, o tamanho da janela TCP, o tempo de vida dos pacotes, entre outras diversas funções que a ferramenta disponibiliza. Acompanhe na Tabela 4 o comando de instalação e execução da ferramenta.

Tabela 4 - Instalação do Hping.

	Comandos Instalação	Comandos Execução
1	*sudo apt-get update*	---
2	*sudo apt-get install hping*3	*hping*3 “parâmetros”

Fonte: Do autor (2016).

O endereço IP foi fornecido quando se criou o servidor vítima, embora existam várias técnicas que podem ser utilizadas para obtenção de endereços IP, cita-se a engenharia social como uma das mais conhecidas. Outra possibilidade de obtenção de endereços IP, é a intermediada por funcionários da própria empresa.

Salienta-se que neste trabalho não foi utilizada qualquer técnica ilícita para obtenção dos recursos necessários para o seu desenvolvimento.

Para execução dos testes, foram utilizados os seguintes recursos com as seguintes características:

a) computador *HP Envy* 2090nr:

- sistema operacional *Windows 10 Pro 64 Bits;*
- processador *Intel Core i7-2630QM CPU 2.00 GHz;*
- armazenamento SSD 256 GB;
- memória *RAM* 8GB,

b) computador *Desktop Lenovo*:

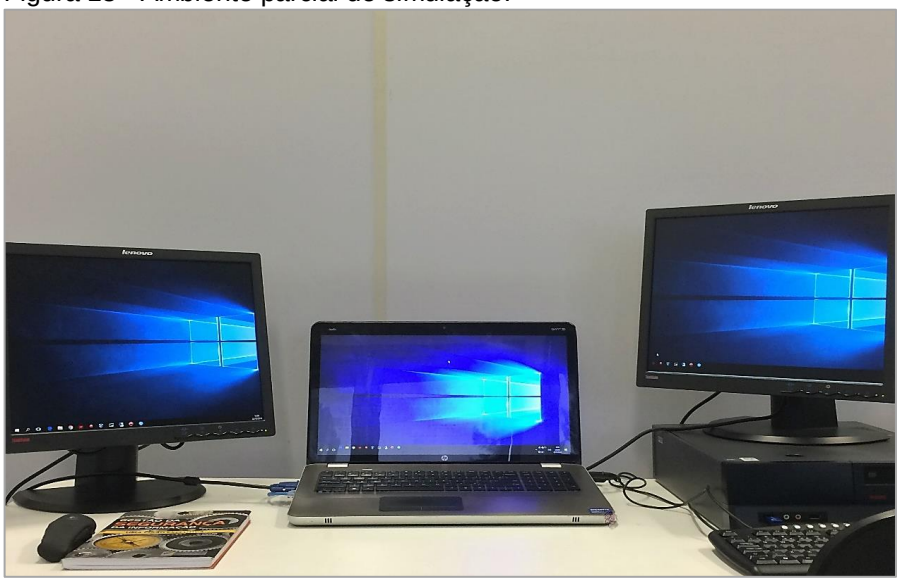
- sistema operacional *Windows 10 Pro 64 Bits;*
- processador *AMD Athlon Dual Core* 5000B 2.60 *GHz;*
- armazenamento *HDD* 325 *GB;*
- memória *RAM* 8 *GB*,

c) conexão à Internet (fibra):

- modem *furukawa ONU*-E200B;
- *switch ethernet* 10/100 Mbps 16 portas;
- taxa de *download* 20 Mbps*;*
- taxa de *upload* 20 Mbps*.*

Na sequência, executou-se o servidor de ataque *Linux Debian* no computador HP. O monitor à esquerda e o computador *Lenovo* à direita, serviram para auxiliar na análise e comportamento dos testes.

Figura 18 - Ambiente parcial de simulação.



Fonte: Do autor (2016).

Uma vez compreendido e configurado todo o cenário de ataque, avançou-se para o cenário de defesa.

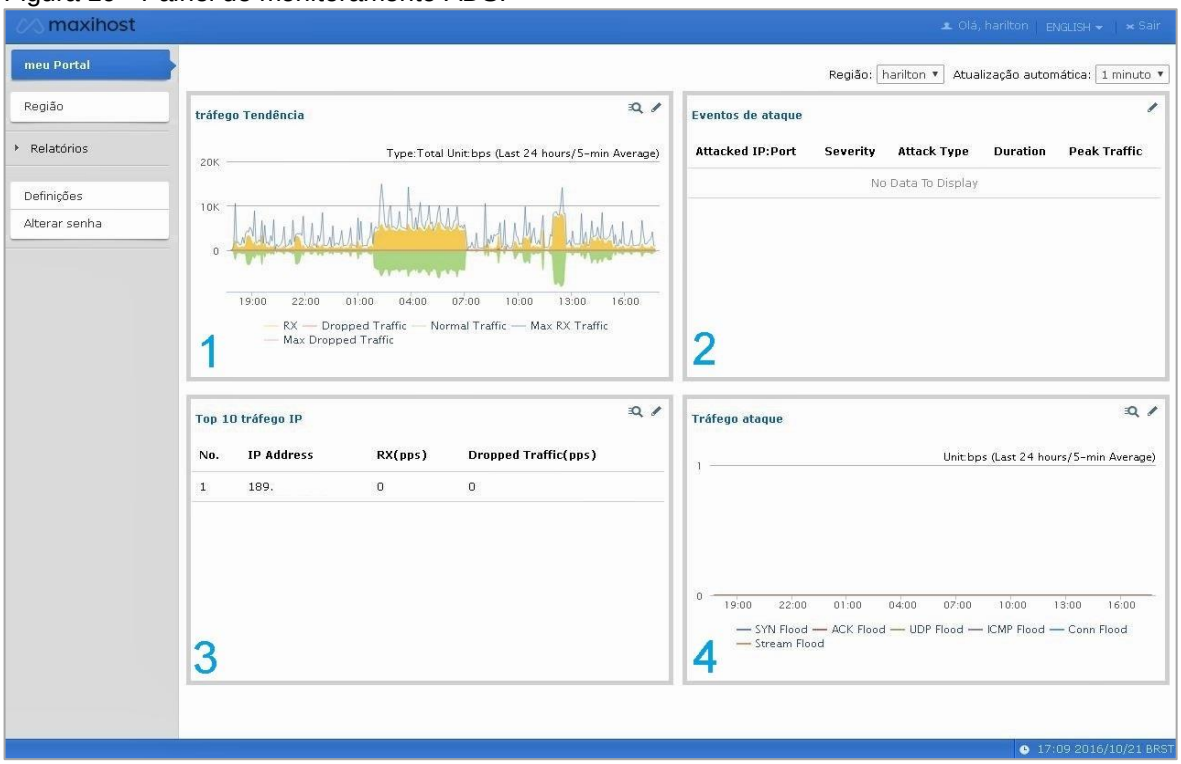
6.4.2 Cenário de defesa

Para que a proteção de ataques DoS da *Maxihost* seja efetiva, a empresa utiliza os equipamentos da *NsFocus* em conjunto com os *softwares* de monitoramento *Nagios*, *Ubersmith*, *Cacti*, *The Dude*, para captura de pacotes, geração de gráficos e alguns dados estatísticos, além de possuir *boots* integrados aos sistemas de *chat* interno (LIMA, 2016).

Como mencionado anteriormente, foi cedido ao acadêmico dois painéis de monitoramento, a saber: o painel *Anti-DoS System Manager (*ADS-M*)*, que permitiu observar o comportamento da rede em tempo real (figura 19), e o painel do servidor da vítima, que permitiu analisar o comportamento da interface de rede, e outras informações a serem descritas no cenário da vítima (figura 22).

Com o uso do painel *Anti-DoS System Manager* foi possível: (1) monitorar o tráfego geral (análise e captura de pacotes), (2) registrar os eventos de ataque (3) verificar o endereço IP da vítima, (4) monitorar o tráfego de ataque (figura 19).

Figura 19 - Painel de monitoramento ADS.



Fonte: *Maxihost* (2016).

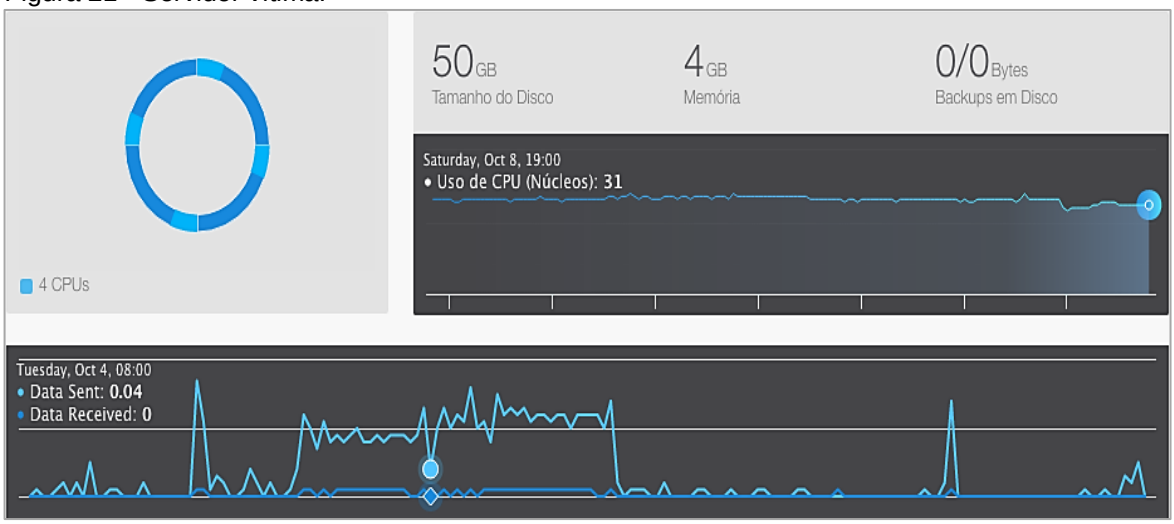
6.4.3 Cenário da vítima

Com a finalidade de comprovar a existência de um ataque DoS, por um lado, e a existência de um sistema de proteção, por outro, criou-se uma vítima que pudesse receber o ataque. Observe-se a seguir algumas das suas características de *software* e *hardware* (figuras 20 e 21).

Figura 20 - Servidor vítima.

Fonte: Adaptado de *Maxihost* (2016).

Figura 21 - Servidor vítima.



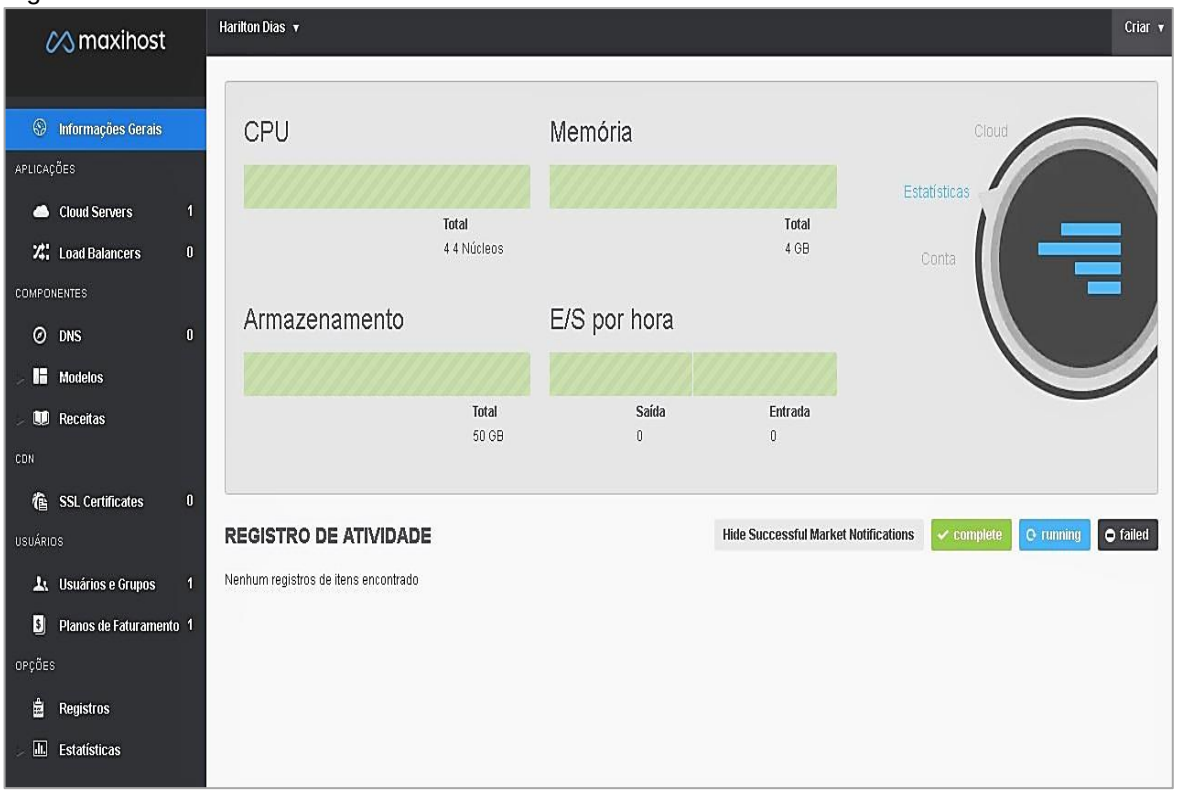
Fonte: *Maxihost* (2016).

Trata-se de um ambiente que simula uma rede com um usuário e tráfego legítimo, pelo menos até não se registrar à ocorrência de um crime digital. O ambiente possui o sistema de monitoramento e mitigação da *Maxihost*.

Na ausência desta tecnologia de proteção, se fosse originado um ataque à esta rede, o serviço ou site estaria total ou parcialmente fora do ar.

O segundo painel de monitoramento (figura 22), foi o responsável por monitorar todas atividades do servidor vítima.

Figura 22 - Painel de monitoramento servidor vítima.



Fonte: *Maxihost* (2016).

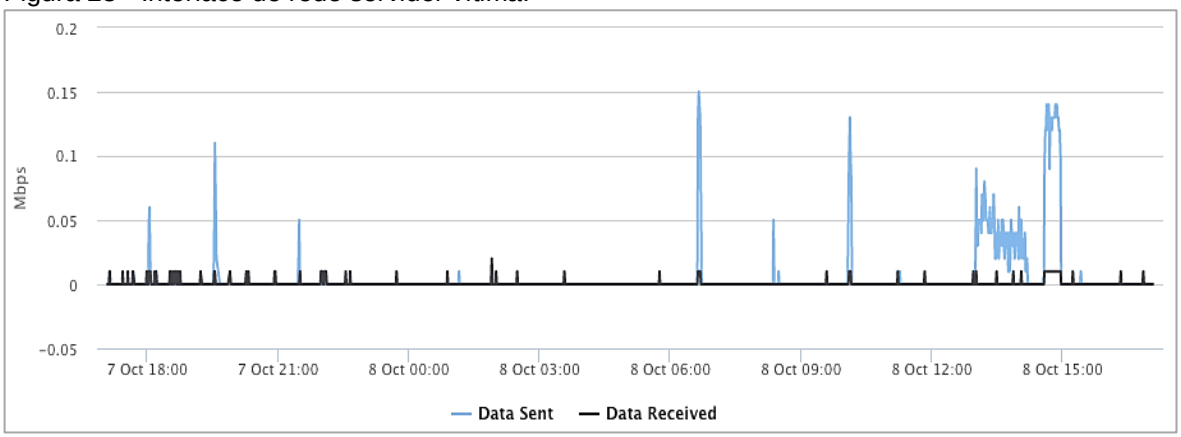
O uso deste painel permitiu acompanhar o comportamento do usuário na rede. No painel estavam contidas todas as características indiciosas e pertinentes a este servidor. Das funções já mencionadas, acrescenta-se ainda a possibilidade de consultarem-se as seguintes informações:

a) certificados de segurança instalados;
b) usuários e grupos;
c) registros;
d) estatísticas;
e) horários de utilização;

f) comportamento do usuário.

A figura 23 apresenta o gráfico de utilização da interface de rede da vítima, com dados recebidos e enviados.

Figura 23 - Interface de rede servidor vítima.



Fonte: *Maxihost* (2016).

Com os cenários preparados e todas ferramentas devidamente instaladas e configuradas, deu-se sequência a etapa final da pesquisa.

6.5 EXECUÇÃO E SIMULAÇÃO DO ATAQUE

Para controle e execução do ataque foram estabelecidas algumas diretrizes:

a) período de execução de ataque (matutino e/ou vespertino);
b) tempo máximo (até 1h);
c) geração de tráfego (malicioso);
d) tipo de ataque (DoS SYN *Flood*).

Como abordado anteriormente, para que uma conexão entre o cliente e o servidor seja aberta, é necessário que exista um pedido *(SYN)*, uma resposta (*SYN-ACK*) e uma confirmação (*ACK*). Com o auxílio do *software hping,* esta simulação descarta a confirmação solicitada pelo servidor, observa-se o comando de execução na tabela 5.

Tabela 5 - Comando de execução *SYN Flood.*

	Comandos Instalação	Comandos Execução
1	---	hping3 -d 1400 -S -w 64 -p 80 --flood 189.x.x.x

Fonte: Dados do próprio autor (2016).

Prosseguindo com a análise da tabela, observa-se alguns parâmetros que carecem de atenção, nomeadamente:

a) ***hping*:** efetua requisições e manipula pacotes TCP/IP;
b) **-d:** define tamanho alocado para cada pacote a ser enviado;
c) **-s:** seta a *flag* para pacotes do tipo SYN;
d) **-w:** define o tamanho da janela;
e) **-p:** indica o número da porta;
f) ***--flood*:** envia o maior número possível de pacotes, sem considerar obter respostas;
g) **189.x.x.x** *host* da vítima.

Existem outros parâmetros que o *hping* utiliza e que são aplicáveis, como por exemplo, o comando *--rand-source*, que permite ocultar o IP e gerar vários outros de forma aleatória. O uso desta expressão permite dificultar a origem do ataque. Outras informações podem ser obtidas na documentação oficial da página <http://www.hping.org/documentation.php> (SANFILIPPO, 2006, tradução nossa).

Para execução dos ataques apenas foram definidos os períodos, podendo a ocorrência acontecer a qualquer hora do dia e sem aviso ou interferência alguma da empresa de proteção.

Ao executar o comando de ataque, passou-se a enviar uma enorme quantidade de requisições de abertura de conexão ao servidor vítima e nunca as responder de volta, tal como ilustra o *log* da tabela 6.

Tabela 6 - Log do ataque gerado pelo *hping*.

```
root@servidordeataque:~# hping3 -d 1400 -S -w 64 -p 80 --flood 189.x.x.x
HPING 189.x.x.x (eth0 189.x.x.x): S set, 40 headers + 1400 data bytes
hping in flood mode, no replies will be shown


--- 189.x.x.x hping statistic ---
28471601 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@servidordeataque:~#
```

Fonte: Do autor (2016).

Prosseguindo com a análise da tabela 6, notou-se que o *hping* forneceu algumas estatísticas sobre a execução do ataque, entre elas a quantidade de pacotes

transmitidos, recebidos e/ou perdidos, assim como os seus respetivos intervalos de ida e volta *(min/avg/max).*

6.6 RESULTADOS OBTIDOS

Os resultados obtidos desta pesquisa, tiveram como embasamento a execução do ataque feito no subcapítulo anterior. Foram coletados dados referente ao mês de outubro.

Os cenários de aplicação, assim como a ferramenta utilizada para realizar o ataque, não sofreram alteração. No entanto, foi utilizado um servidor virtual local para originar o ataque e não o servidor VPS.

Ao utilizar o servidor local para gerar o ataque foi possível obter uma maior quantidade de tráfego malicioso, facilitando a compreensão e a visualização dos tipos de tráfegos detectados.

Como mencionado anteriormente, os únicos sistemas que tiveram interferência do acadêmico foram os de ataque, e o servidor da vítima (para geração do tráfego legítimo). Para o sistema de defesa, foram apenas disponibilizados painéis de monitoramento.

A primeira etapa, consistiu em acessar remotamente a vítima. O objetivo foi de simular o comportamento que um usuário legítimo da rede teria. Este por sua vez, realizava as suas atividades de rotina, acessando algumas páginas, o *streaming* de um vídeo, e o *download* de um arquivo no formato *ISO.*

Na tabela 7 foram listadas as URLs correspondentes às páginas acessadas momentos antes de ser originado o ataque.

Tabela 7 - URLs das páginas acessadas pelo servidor vítima.

URLs
http://www baixaki.com.br
https://www.google.com.br
http://www.unesc.net/portal/
http://www.maxihost.com.br
http://www tecmundo.com.br
https://www.youtube.com/watch?v=pAKojeLTe3E
http://cdimage.debian.org/debian-cd/8.6.0/amd64/iso-cd/debian-8.6.0-amd64-CD-1.iso

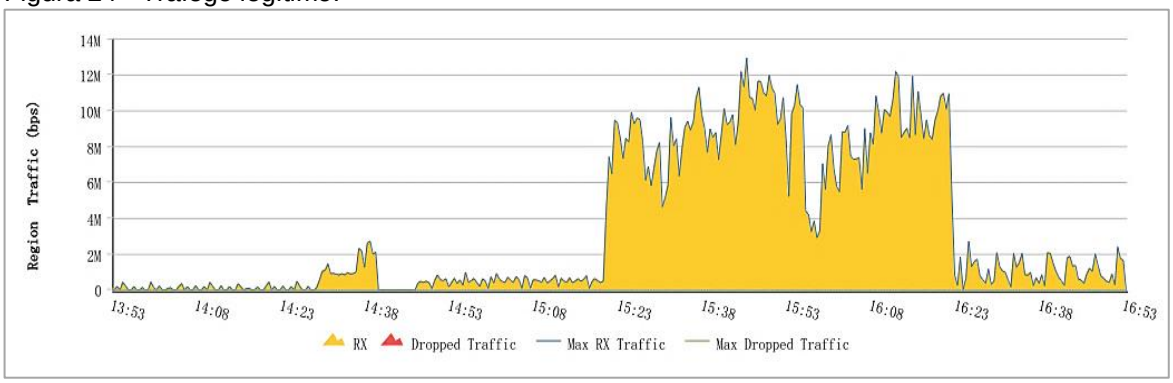
Fonte: Do autor (2016).

As etapas seguintes, consistiram na análise e comportamento do ataque DoS controlado, com o auxílio do painel de monitoramento ADS-M, foram exportadas as informações pertinentes ao evento.

O gráfico da figura 24 foi umas das primeiras informações a serem extraídas. Trata-se de um gráfico de área que destaca os picos de tráfego legítimo da rede em uma média de 30 segundos numa relação “bps (*bits per second*) x tempo”. Foi registrado um pico máximo de 13 Mbps de volume de tráfego legítimo.

Vale ressaltar, que os valores de tráfego gerados foram suficientes para obter os resultados desta pesquisa, portanto, não houve a necessidade de ampliar tanto o volume de tráfego legítimo quanto ao volume de tráfego malicioso.

Figura 24 - Tráfego legítimo.



Fonte: *Maxihost* (2016).

Prosseguindo com a análise da figura 24, durante a exportação do gráfico foram aplicados alguns filtros como, região, porta, e endereço IP. Foi possível também gerar e visualizar separadamente o gráfico em quatro modos, (1) RX, tráfego recebido, (2) *Dropped Traffic*, tráfego perdido, (3) *Max RX Traffic*, quantidade máxima de tráfego recebido, e (4) *Max Dropped Traffic*, quantidade máxima de tráfego perdido.

Com o ataque iniciado, o sistema foi capaz de identificar e encaminhar o IP para o centro de mitigação num intervalo de 30 a 50 segundos. O evento registrou a origem do ataque, a severidade, o tipo, a duração, e o pico de tráfego malicioso gerado (tabela 8).

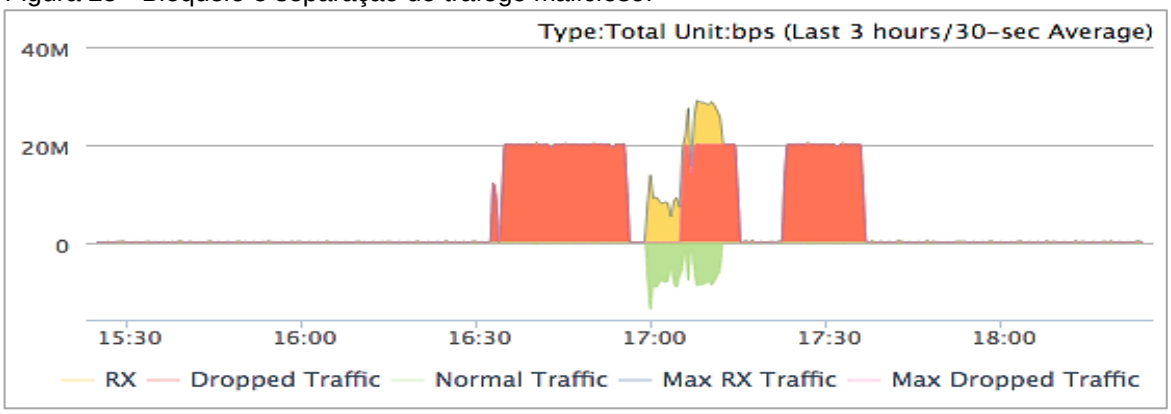
Tabela 8 - Eventos de ataque.

IP : Porta	Severidade	Tipo de Ataque	Duração	Pico de Tráfego
189.x.x.x:80		SYN *Flood*	16 min(s) 30 seg	1.7 Kpps/20.0 Mbps

Fonte: Adaptado de *Maxihost* (2016).

Na sequência, verificou-se no gráfico da figura 25 o comportamento do tráfego malicioso gerado pelo ataque. Nesta ocasião, constatou-se um tráfego legítimo (marcado em amarelo) de 29 Mbps.

Figura 25 - Bloqueio e separação do tráfego malicioso.



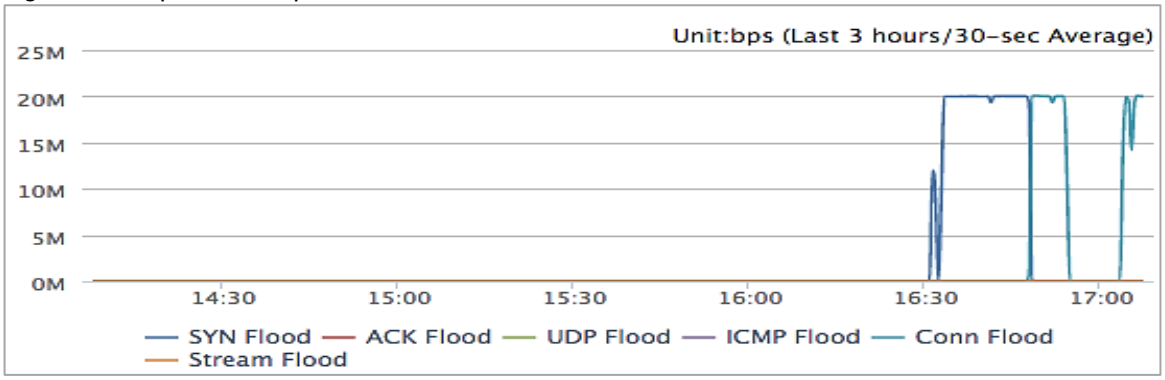
Fonte: *Maxihost* (2016).

Observou-se na figura o aparecimento de tráfego malicioso (marcado a vermelho), originado do ataque de inundação SYN *Flood,* que teve início aproximadamente às 16h33min e com um total de 20 Mbps.

Com o aparecimento do tráfego malicioso, o sistema passou a classificar o gráfico em cinco modos de visualização, dos quais, quatro já foram esclarecidos anteriormente. Diferente do anterior, surgiu o modo de visualizar apenas o tráfego normal (*normal traffic*), constituindo este a média calculada pelo sistema, de acordo com comportamento do usuário.

A figura 26 e figura 27 complementam a explicação, exibindo gráficos exclusivos que registram os vários tipos de ataques de inundação. A figura 26, em particular, aponta o início do ataque e o seu comportamento.

Figura 26 - Tipos de ataque.

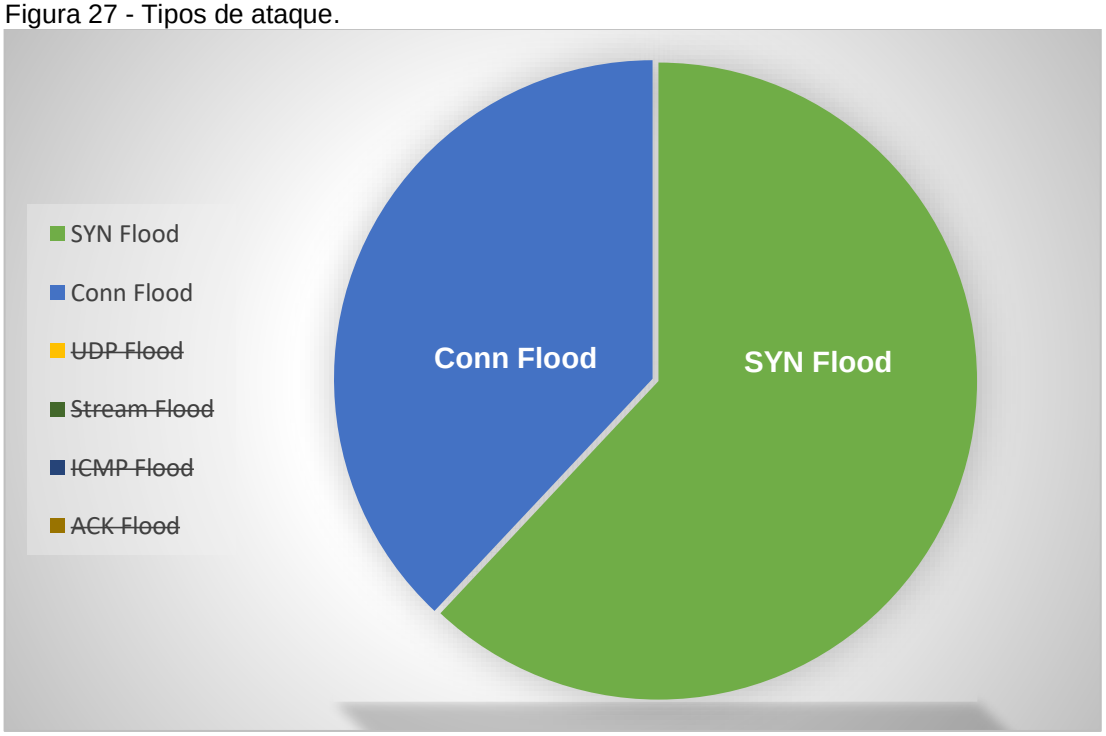


Fonte: *Maxihost* (2016).

O sistema de proteção da *Maxihost* possui uma *blacklist*, que identifica se o IP está a enviar pacotes (não padrão) para o endereço IP protegido. Desta forma, o sistema considera que o IP representa uma ameaça para a estrutura e o bloqueia-o automaticamente por uma semana, é o que aponta um dos engenheiros de segurança da empresa (LIMA, 2016).

Analisando o gráfico da figura 26, foi possível observar o exato momento que o sistema passou a considerar o IP de ataque como um risco para a estrutura. O número de tentativas feitas pelo mesmo endereço, foi uma das características que o sistema utilizou para bloqueá-lo. A ação pode ser observada quando o comportamento da onda do gráfico mudou para o ataque do tipo *Conn Flood,* precisamente às 16h50min.

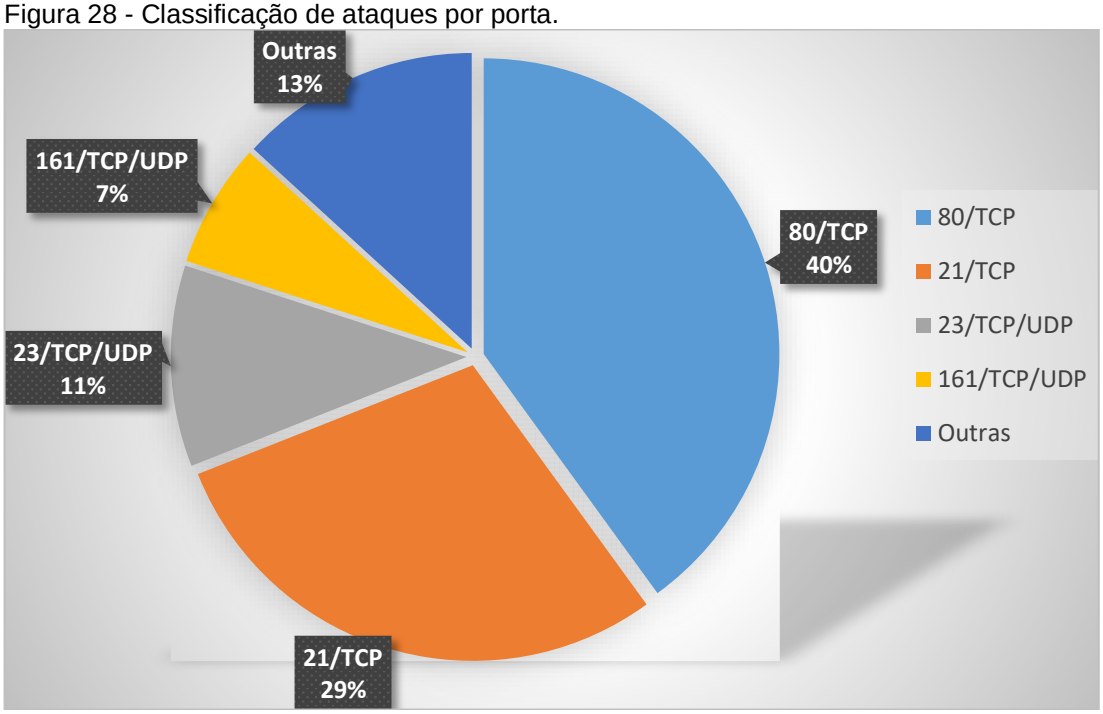
Figura 27 - Tipos de ataque.



Fonte: Adaptado de *Maxihost* (2016).

Na fase seguinte, analisou-se na figura 28 a classificação dos ataques, apontando as portas e os protocolos que foram alvos.

Figura 28 - Classificação de ataques por porta.



Fonte: Adaptado de *Maxihost* (2016).

Observou-se nas amostragens, uma maior incidência dos ataques no protocolo TCP direcionado para as portas 80 e 21, resultando num total de 69%. E para o protocolo UDP as portas 23 e 161, com um total de 18%. Os restantes 13%, foram direcionados para diferentes portas em ordem crescente quando foi adicionado no comando de ataque (tabela 5) o operador ++ antes do número da porta (*-p ++80*).

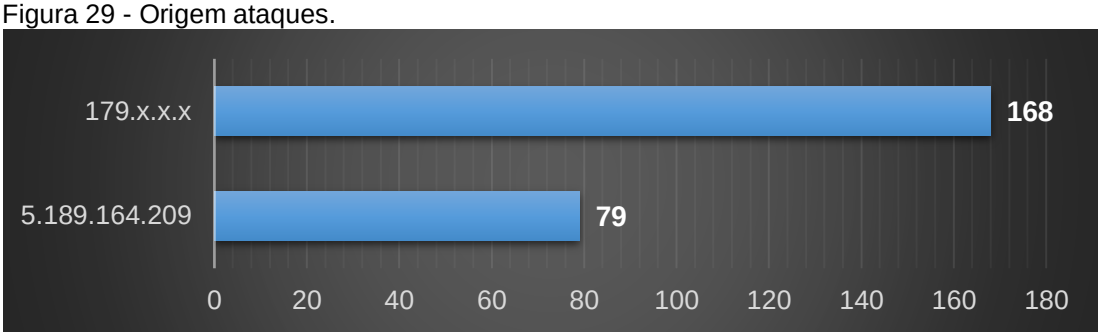
Na sequência, a tabela 9 e a figura 29 apontaram o número de vezes que o IP apareceu na lista de fontes. Os dados das figuras provêm da amostragem entre estatísticas de pacotes de ataque.

Tabela 9 - Contagem de ataques.

Nº	IP de Ataque	Data	Frequência
1	179.x.x.x (Servidor *Debian*)	2016-10-24 16:47:00	168
3	5.189.164.209 (VPS)	2016-10-24 15:30:01	79

Fonte: Adaptado de *Maxihost* (2016).

Figura 29 - Origem ataques.



Fonte: Adaptado de *Maxihost* (2016).

Na etapa final, exibe-se os dados estatísticos sobre o tráfego geral da rede (tabela 10).

Tabela 10 - Estatísticas tráfego da rede.

Time	Tráfego Recebido (RX)		Tráfego Perdido	
	Med (bps/pps)	Max (bps/pps)	Med (bps/pps)	Max (bps/pps)
2016-10-01	848 / 1	25.4K / 35	0 / 0	80 / 0
2016-10-02	1.3K / 2	22.8K / 32	1 / 0	96 / 1
2016-10-03	3.2K / 4	992.9K / 88	2 / 0	1.8K / 4
2016-10-04	4.1K / 6	26.7K / 38	1 / 0	80 / 1
2016-10-05	1.9K / 2	20.5K / 28	1 / 0	96 / 1
2016-10-06	860 / 1	11K / 15	2 / 0	4.3K / 9
2016-10-07	1.1K / 1	15.4K / 15	1 / 0	424 / 1
2016-10-08	899 / 1	43.2K / 17	1 / 0	416 / 1
2016-10-09	814 / 0	13.7K / 17	0 / 0	72 / 1
2016-10-10	934 / 1	13.6K / 13	0 / 0	72 / 0
2016-10-11	1.3K / 1	375.2K / 52	1 / 0	72 / 0
2016-10-12	1.7K / 2	16.6K / 20	0 / 0	360 / 1
2016-10-13	1.4K / 1	14.8K / 19	21 / 0	360 / 1
2016-10-14	1.8K / 2	22.2K / 26	1 / 0	64 / 0
2016-10-15	992 / 1	15.5K / 19	1 / 0	72 / 1
2016-10-16	1.5K / 2	18.6K / 27	1 / 0	80 / 0
2016-10-17	1.2K / 1	51.1K / 30	1 / 0	688 / 1
2016-10-18	85.4K / 16	3.0M / 752	0 / 0	72 / 1
2016-10-19	195.0K / 37	40.7M / 4.1K	29.6K / 4	20.0M / 2.9K
2016-10-20	18.2K / 6	1.2M / 199	1 / 0	72 / 1
2016-10-21	2.0K / 2	14.9K / 18	2 / 0	392 / 1
2016-10-22	6.1K / 7	19.6K / 25	30 / 0	344 / 1
2016-10-23	10.0K / 14	23.8K / 25	1 / 0	96 / 1
2016-10-24	1.2M / 160	29.0M / 3.2K	628.9K / 54	20.1M / 1.7K
2016-10-25	97.1K / 32	3.6M / 326	1 / 0	80 / 1
2016-10-26	56.5K / 20	2.8M / 245	1 / 0	144 / 1
2016-10-27	970 / 0	224.4K / 20	1 / 0	96 / 1
2016-10-28	1.6K / 2	17.3K / 23	1 / 0	128 / 1
2016-10-29	1.3K / 1	25.6K / 24	1 / 0	192 / 0
2016-10-30	859 / 1	41.1K / 24	1 / 0	64 / 1

Fonte: Adaptado de *Maxihost* (2016).

Com os dados estatísticos do tráfego geral da rede, extraídos a partir do painel ADS-M, foi possível identificar que:

a) o pico máximo de tráfego legítimo atingiu 40.7 Mbps, precisamente no dia 19 de outubro;
b) o pico máximo de tráfego malicioso ocorreu no dia 24 e atingiu 20.1 Mbps, sendo cerca de 10% de tráfego legítimo comprometido;
c) o protocolo TCP direcionado à porta 80 (serviço *world wide web*), foi um dos protocolos de comunicação que mais sofreu incidência do ataque, seguindo o protocolo UDP;
d) o tráfego malicioso foi separado do tráfego legítimo sem comprometer o servidor.

Com os dados obtidos, foi possível interpretar que a execução do ataque DoS, quando não identificado, provê uma taxa de êxito muito alta, principalmente na ausência de uma ferramenta ou serviço capaz de mitigar a ameaça.

7 CONCLUSÃO

Vivenciamos uma era que está totalmente voltada para a tecnologia de informação. Passamos a manipular e a armazenar as nossas informações em centenas de dispositivos de diferentes arquiteturas.

Toda esta evolução tem despertado o interesse de entusiastas e, se por um lado, alguns destes focam-se em estudar estas novas tecnologias como contributo para o seu próprio conhecimento, ou para auxiliar a comunidade em geral, outros estudam-na para tirarem proveito e vantagem, agindo sem ética nem índole.

Este trabalho evendiciou algumas das principais ameaças da atualidade, em particular os ataques de negação de serviço. Observou-se o comportamento e a influência que estas ameaças em geral manifestam perante o ativo mais valioso da sociedade, a informação.

Notou-se também, que o aumento constante de meios de comunicação, serviços e tipos de dispositivos utilizados, proporcionam consideravelmente o aumento de crimes digitais.

Para que se pudesse propor uma solução adequada de proteção, foi fundamental antes de mais nada, aplicar um estudo de caso, onde foi executado um ataque DoS, permitindo desta forma, entender e analisar o comportamento da ameaça. Como resultado, adquiriu-se o conhecimento necessário para a realização do ataque, seguindo da aplicação da contramedida de mitigação baseada na *cloud computing.* No final, fez-se a devida análise dos dados e documentou-se os resultados obtidos.

O termo *cloud computing* surgiu há um bom tempo, tal como já foi visto anteriormente no Capítulo 4. Todavia, o termo só passou a ganhar mais força no mercado perto de 2008. A sua essência permitiu abrir um leque de possibilidades para o mercado, deixando assim de ser apenas uma tendência, e sim uma necessidade para as organizações lidarem e sobreviverem com a concorrência. Mas como qualquer outra nova tecnologia, o seu passado levantou algumas dúvidas pertinentes à sua segurança, estariam as empresas seguras ao alocar as suas informações e ao utilizar os seus serviços. A ocorrência de alguns problemas chegou até mesmo a levantar questionamentos sobre a sua duração, mas com o passar dos anos, esta tecnologia recebeu e ainda recebe diversos investimentos para cumprir com a sua promessa, a de revolucionar o modo de armazenamento e manuseio da informação.

Hoje, a *cloud computing* tem um posicionamento diferente no mercado e, certamente aprendeu com os erros do passado. E foi diante deste contexto, que se escolheu para esta pesquisa, a solução de monitoramento e proteção baseada na *cloud*.

No decorrer desta pesquisa foram encontradas algumas dificuldades, sendo estas resolvidas posteriormente, permitindo deste modo a apresentação e aplicação da solução proposta.

Umas das dificuldades encontradas, se não, a que maior grau de dificuldade apresentou, foi sobre a impossibilidade de realizar uma conexão direta com a empresa, em razão da inviabilidade e por suplantarem os limites financeiros do acadêmico. Todavia, esta situação foi contornada quando se pensou em criar a vítima dentro da própria empresa.

Outro problema encontrado foi o de gerar uma taxa considerável de tráfego malicioso. Após várias pesquisas, o problema foi resolvido ao aprimorar a técnica de ataque, incluindo um parâmetro adicional a sintaxe no comando de execução.

Superadas todas as dificuldades, em particular as que mais tiveram destaque, foi possível dar continuidade ao desenvolvimento do trabalho proposto.

Para o desenvolvimento desta pesquisa e para sua orientação, foram estabelecidos seis objetivos específicos e um objetivo geral. No final, estes objetivos foram alcançados com sucesso quando se obteve o conhecimento acerca dos sistemas de informação (v. Capítulo 1), acerca dos protocolos de comunicação e acerca das atuais ameaças que têm surgido – sobretudo os ataques DoS (v. Capítulo 3), acerca da contramedida de mitigação abordada (v. Capítulo 4) e acerca do cenário de aplicação e resultados obtidos (v. Capítulo 6).

Desta forma, acredita-se que uma vez alcançados os objetivos específicos delimitados no início da pesquisa, alcançou-se de igual forma o objetivo geral do trabalho, o de monitorar e aplicar uma contramedida de mitigação contra-ataques de negação de serviço baseada na *cloud computing*.

O sistema de proteção da *Maxihost* mostrou ser uma solução inovadora e com diversas características peculiares. A solução reúne recursos necessários para manter as propriedades básicas da segurança preservadas. É importante saber que os sistemas atuais de proteção não foram projetados para lidarem com ataques DDoS. Portanto, a implantação de uma solução dedicada e exclusiva para este tipo de

ameaças, é essencial para complementar um ambiente totalmente seguro e capaz de manter o ativo mais valioso da sociedade em segurança.

Em suma, o presente trabalho conheceu o seu êxito quando comprovou que os ataques DoS representam umas das maiores ameaças da atualidade. Cada vez mais, crescem, tornam-se comuns, e aumentam os riscos a que as instituições e empresas estão expostas. Ainda assim, observa-se uma certa resistência de algumas instituições e empresas em aderirem a soluções de proteção baseadas na *cloud computing*. Talvez os erros do passado da *cloud computing* estejam a influenciar nesta tomada de decisão, ou talvez ainda exista outras razões. Fato é, que todos estes questionamentos e dúvidas abrem portas para futuros trabalhos.

Desta forma, propõe-se um estudo sobre as razões que levam às instituições e empresas a resistirem à migração e contratação de serviços baseados na *cloud computing*, fica como outra sugestão, a implantação de uma *cloud* local privada, que adote soluções de monitoramento e proteção, eliminando-se, desta forma, a necessidade exclusiva de contratar uma empresa que forneça a solução.

REFERÊNCIAS

ABNT NBR ISO/IEC 27002. **Tecnologia da Informação, Técnicas de Segurança:** código de prática para gestão da segurança da informação. Associação Brasileira de Normas Técnicas, 2013. Disponível em: <http://www.abntcatalogo.com.br/norma.aspx?ID=306582>. Acesso em: 4 mar. 2016.

ABNT NBR ISO/IEC 27005. **Tecnologia da Informação, Técnicas de Segurança:** código de prática para gestão da segurança da informação. Associação Brasileira de Normas Técnicas, 2011. Disponível em: <http://www.abntcatalogo.com.br/norma.aspx?ID=089327>. Acesso em: 20 jan. 2016.

ADDED. **Soluções em Tecnologia da Informação, 2014.** Disponível em: <http://www.added.com.br/news/saas-paas-iaas/>. Acesso em: nov. 2015.

AMARANTE, Sílvio, R. Martins. **Utilizando o Problema de Múltiplas Mochilas para Modelar o Problema de Alocação de Máquinas Virtuais em Computação nas Nuvens, 2013.** Dissertação (Mestrado em Ciência da Computação). Disponível em: <http://goo.gl/7sbsU8>. Acesso em: 6 ago 2016.

ALQAHTANI, Saeed M; BALUSHI, Al; JOHN, Robert. **An Intelligent Intrusion Prevention System for Cloud Computing (SIPSCC), 2014**. [Artigo IEEE Xplore Digital Library]. Disponível em: <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6822321&newsearch=true&queryText=Intrusion%20prevention%20systems%20on%20cloud%20>. Acesso em: 25 maio 2016

ASHFORD, Warwick. **More Action Needed to Stop NTP DDoS Attacks, says Report, 2014.** Disponível em: <http://www.computerweekly.com/news/2240223221/More-action-needed-to-stop-NTP-DDoS-attacks-says-report>. Acesso em: 19 jun. 2016.

DICTIONARY CAMBRIDGE. **Definition Checksum, 2016.** Disponível em: <http://dictionary.cambridge.org/pt/dicionario/ingles/checksum>. Acesso em: 8 jun. 2016.

ARMBRUST, Michael et al. **Above the Clouds:** a Berkeley view of cloud computing, 2009. Disponível em: <https://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf>. Acesso em: 12 jun. 2016.

BASTA, Alfred. **Glossário:** bootnets, hacktivismo. São Paulo: Cengage Learning, 2014.

_____. **Segurança de computadores e teste de invasão.** São Paulo: Cengage Learning, 2014.

BEAVER, Kevin. **How Can the SSDP Protocol be Secured to Provent DDoS Attacks, 2015.** Disponível em: <http://searchsecurity.techtarget.com/answer/How-

can-the-SSDP-protocol-be-secured-to-prevent-DDoS-attacks >. Acesso em: 25 set. 2016.

BIGELOW, Stephen J. **Create a Cloud DDoS Protection Plan, 2016.** Disponível em: <http://searchcloudcomputing.techtarget.com/tip/Create-a-cloud-DDoS-protection-plan >. Acesso em: 20 set. 2016.

BLEVINS, Brandan. **NTP-based DDoS Attacks on the Rise, but SYN Floods Still more Perilous, 2014.** Disponível em: <http://searchsecurity.techtarget.com/news/2240217471/NTP-based-DDoS-attacks-on-the-rise-but-SYN-floods-still-more-perilous>. Acesso em: 4 mar. 2016.

BLACK HAT. **About us, 2016.** Disponível em: <https://www.blackhat.com/about.html>. Acesso em: 20 set. 2016.

_____; WU, Erik. **Dark Side of The DNS Force, 2016.** Disponível em: <https://www.blackhat.com/docs/us-16/materials/us-16-Wu-Dark-Side-Of-The-DNS-Force.pdf>. Acesso em: 20 set. 2016.

CASTRO, Rita de C. C de; SOUSA, Verônica L. Pimental de. **Segurança em Cloud Computing:** Governança e Gerenciamento de Riscos de Segurança, 2011. Disponível em: <http://www.infobrasil.inf.br/userfiles/26-05-S5-1-68740-Seguranca%20em%20Cloud.pdf>. Acesso em: 4 ago 2016.

CAPITANGO, Miguel Kapingala. **Segurança na Internet das coisas, 2011**. Disponível em: <http://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2011_2/miguel/index.html>. Acesso em: 29 mar. 2016.

CARISSIMI, Alexandre da Silva; ROCHOL, Jurgen; GRANVILLE, Lisandro Zambenedetti. **Redes de Computadores**. Porto Alegre: Artmed, 2009.

CARNEIRO, Alberto. **Auditoria e Controlo de Sistemas de Informação**. Lisboa: FCA, 2009.

CASCARINO, Richard E. **Auditor's Guide to IT Auditing**. 2. ed. New Jersey: John Wiley & Sons, 2012.

CERT.br. Centro de Estudos, Resposta e Tratamento de Incidentes no Brasil. **Glossário:** malware, vulnerabilidade, incidente, antispam, antispyware, antiphihing, 2012a. Disponível em: <http://cartilha.cert.br/glossario/>. Acesso em: 26 abr. 2016.

_____. Centro de Estudos, Resposta e Tratamento de Incidentes no Brasil. **Sobre o CERT.br, 2012b.** Disponível em: <http://www.cert.br/sobre/>. Acesso em: 25 mar. 2016.

_____. **Incidentes Reportados ao CERT.br:** janeiro a dezembro, 2015. Disponível em:<http://www.cert.br/stats/incidentes/>. Acesso em: 26 abr. 2016.

_____. **Recomendações para Melhorar o Cenário de Ataques Distribuídos de Negação de Serviço (DDoS), 2016.** Disponível em: < http://www.cert.br/docs/whitepapers/ddos/#5>. Acesso em: 26 abr. 2016.

_____. **Incidentes Reportados ao CERT.br:** Janeiro a Dezembro. 2015b. Disponível em: <http://www.cert.br/docs/whitepapers/dns-recursivo-aberto/>. Acesso em: 26 abr. 2016.

CERT.org. **TCP SYN Flooding and IP Spoofing Attacks, 2000.** Disponível em: <http://www.cert.org/historical/advisories/CA-1996-21.cfm>. Acesso em: 20 mar. 2016.

CÉLESTIN, Daniel Paula Pessôa. **Customização do Monitoramento de Links e Redes, 2013**. Disponível em: <http://hdl.handle.net/235/4904>. Acesso em: 02 jun. 2016.

CICHONSKI, Paul; MILLAR, Tom; GRANCE, Tim, SCARFONE, Karen. Computer **Incident Handling Guide, 2012:** recommendations of the national institute of standards and technology. Disponível em: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>. Acesso em: 25 jun. 2016.

COMER, Douglas E. **Redes de Computadores e Internet.** 6. ed. Porto Alegre: Bookman, 2016.

DANTAS, Marcus Leal. **Segurança da Informação:** uma abordagem focada em gestão de riscos. Pernambuco: Olinda, 2011.

EARLS, Alan R. **PaaS, Present and Future:** how containers evolve PaaS frameworks, 2016. Disponível em: <http://searchcloudcomputing.techtarget.com/tip/PaaS-present-and-future-How-containers-evolve-PaaS-frameworks>. Acesso em: 12 ago. 2016.

GUIMARÃES, Dilva; Cabral, Paulo. **Significado de Byte, 2016.** Disponível em: <https://www.significados.com.br/sobre/>. Acesso em: 10 jun. 2016.

INFORMATION SCIENCES INSTITUTE. **RFC 791.Internet Protocol (IP), 1981.** Disponível em: <https://tools.ietf.org/html/rfc791>. Acesso em: 8 ago. 2016.

FAVARO, Anderson. **Instalação do Debian no VirtualBox.** Disponível em: <http://pt.slideshare.net/favaro/instalao-do-debian-no-virtualbox>. Acesso em: 15 set. 2016.

FERNANDES, Aguinaldo Aragon; ABREU, Vlademir Ferraz de. **Implantando a Governança de TI da Estratégia à Gestão dos Processos e Serviços.** 2014. 4. ed. Rio de Janeiro: Brasport, 2014.

FEY, Ademar Felipe. **Introdução à Comunicação de Dados e Redes de Computadores.** São Paulo: Amazon Digital Services, 2016.

FILHO, João Eriberto Mota. **Descobrindo o Linux:** entenda o sistema operacional Gnu/Linux. 3. ed. São Paulo: Novatec, 2013.

FRASER, B. **Site Security Handbook, 1997**. Tradução nossa: RFC 2196. Disponível em: <http://penta.ufrgs.br/gereseg/rfc2196/>. Acesso em: 3 jan. 2016.

GATES, Bill. **A estrada do futuro.** São Paulo: Companhia das Letras, 1995.

GOMES, Carina Nobre. **Estudo do Paradigma Computação em Nuvem.** Dissertação de Mestre [Repositório Politécnico de Lisboa, 2012]. Disponível em: <http://repositorio.ipl.pt/handle/10400.21/2375>. Acesso em: 8 ago. 2016.

HELLER, Michael. **More DDoS DNS Amplification Attacks use SSDP than NTP, 2016.** Disponível em: <http://searchsecurity.techtarget.com/news/450302279/More-DDoS-DNS-amplification-attacks-use-SSDP-than-NTP>. Acesso em: 20 jun. 2016.

HOFFMAN, Stefanie. **DDoS:** A brief History, 2013. Disponível em: <https://blog.fortinet.com/2013/03/25/ddos-a-brief-history>. Acesso em: 27 jun. 2016.

INCAPSULA INC. **Denial of Service Attacks, 2016.** Disponível em: <https://www.incapsula.com/ddos/ddos-attacks/denial-of-service.html>. Acesso em: 27 maio 2016.

_____. **2013-2014 DDoS Threat Landscape Report.** Disponível em: <https://lp.incapsula.com/rs/incapsulainc/images/2013-14_ddos_threat_landscape.pdf>.Acesso em: 30 fev. 2016.

KUNDRA, Vivek. **Federal Cloud Computing Strategy.** Disponível em: <http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf>. Acesso em: 29 maio 2016.

KUROSE, James F. **Redes de Computadores e a Internet:** uma abordagem top-down. 5ª ed. São Paulo: Addison Wesley, 2010.

LAUDON, Kenneth C; LAUDON, Jane P. **Sistemas de informação Gerenciais.** 11ª ed. São Paulo: Pearson Education, 2014.

LYRA, Maurício Rocha. R. **Segurança e Auditoria em Sistemas de Informação.** Rio de Janeiro: Ciência Moderna, 2008.

_____. **Governança da Segurança da Informação**. Brasília, 2015.

MAXIHOST. **Monitoramento, 2016a.** Disponível em: <http://maxihost.com.br/servicos-gerenciados/monitoramento/>. Acesso em: 5 jun. 2016.

_____. **Sobre nós, 2016b.** Disponível em: <http://maxihost.com.br/sobre/>. Acesso em: 5 jun. 2016.

_____. **Proteção DoS e DDoS, 2016c**. Disponível em: <http://maxihost.com.br/protecao-ddos/>. Acesso em: 5 jun. 2016.

_____. **Ficha de Dados, 2016d.** Disponível em: <http://cdn2.hubspot.net/hubfs/1772761/DDoS_Protection/Datasheet_DDoS_Portugues.pdf>. Acesso em: 6 jun. 2016.

MICROSOFT. **The Security Risk Management Guide Microsoft, 2006.** Disponível em: <https://www.microsoft.com/en-us/download/details.aspx?id=6232>. Acesso em: 28 abr. 2016.

MICHAEL, Armbrust et al. **Above the Clouds:** A Berkeley View of Cloud Computing. Disponível em: <http://radlab.cs.berkeley.edu/publication/285>. Acesso em: 8 ago. 2016.

MICHELIN, Régio Antonio. **Mitigação de Ataques de Negação de Serviço em Rests Autenticáveis na Nuvem, 2015.** Disponível em: <http://tede2.pucrs.br/tede2/bitstream/tede/5272/1/465167.pdf>. Acesso em: 2 dez. 2016.

MIRKOVIC, Jelena et al. **Benchmarks for DDOS Defense Evaluation, *2006.*** Artigo [The IEEE *Xplore* Digital Library]. Disponível em: <http://ieeexplore.ieee.org/document/4086729/>. Acesso em: 15 out. 2016.

NETO, José António de Moura. **A Computação em Nuvem para as Micro e Pequenas Empresas, 2011.** Disponível em: <http://www.administradores.com.br/artigos/economia-e-financas/a-computacao-em-nuvem-para-as-mpes/51444/>. Acesso em: 10 ago. 2016.

NEXUSGUARD. **DDoS Threat Report Reflection Attacks Q1 2016.** Disponível em: <https://goo.gl/8c7K1U>. Acesso em: 20 abr. 2016.

NIC.br. **CERT.br registra aumento de ataques de negação de serviço em 2014**. Disponível em: <http://nic.br/noticia/releases/cert-br-registra-aumento-de-ataques-de-negacao-de-servico-em-2014/>. Acesso em: 3 jun. 2016.

NIST. **The NIST Definition of Cloud Computing, 2011**. Disponível em: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>. Acesso em: 20 maio 2016.

NIST. **NIST Cloud Computing Standards Roadmap, 2013**. Disponível em: <http://www.nist.gov/itl/cloud/upload/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf>. Acesso em: 3 ago. 2016.

NOLLE, Tom. **Network Traffic Management Targets Access and Middle Mile:** aggregation Infrastructure, 2009. Disponível em: <http://searchtelecom.techtarget.com/tip/Network-traffic-management-targets-access-and-middle-mile-aggregation-infrastructure>. Acesso em: 1 jun. 2016.

NSFOCUS. **Anti-DDoS System White Paper, 2014.** Disponível em: <http://www.nvc.co.jp/pdf/product/nsfocus/NSFOCUS_ADS_WhitePaper.pdf>. Acesso em: 12 abr. 2016.

OPEN GROUP. The Open Group Guide. **Cloud Computing for Business.** San Francisco: The Open Group, 2011.Disponível em: <http://www3.opengroup.org/news/press/cloud-computing-for-business>. Acesso em: 13 jun. 2016.

OPUS Software. **Computação em nuvem**. 1. ed. São Paulo: OPUS Software Ltda, 2015.

PASCUCCI, Matthew. **Preventing a Distributed Denial-of-Service Attack:** is hardware needed, 2013. Disponível em: <http://searchsecurity.techtarget.com/answer/Preventing-a-distributed-denial-of-service-attack-Is-hardware-needed>. Acesso em: 29 maio 2016.

PEREIRA, Diego da Silva; DANTAS, Alexandre Henrique; MEDEIROS, Harrison Gustavo Silva de. **Análise do Comportamento de um Ataque de Negação de Serviço via SYN-FLOOD a um Servidor Web.** 2012. Disponível em: <http://propi.ifto.edu.br/ocs/index.php/connepi/vii/paper/viewFile/5065/1000>. Acesso em: 25 maio 2016.

PEREIRA, João Paulo Aragão. **Método de Mitigação Contra Ataques de Negação de Serviço Distribuídos Utilizando Sistemas Multiagentes.** 2014. Disponível em: <http://www.teses.usp.br/teses/disponiveis/3/3141/tde-18032015-155642/pt-br.php>. Acesso em: 2 abr. 2016.

PEREIRA, Adan Lucio et al. **Cloud Computing: Information Security in Cloud Environments and Physical Networks, 2016.** Artigo Científico (Revista Brasileira de Engenharia de Produção - BJPE). Disponível em: <http://www.periodicos.ufes.br/BJPE/article/view/EO02_2016/pdf>. Acesso em: 10 ago. 2016.

PEIXOTO, Maycon L. Maciel. **Oferecimento de QoS para computação em nuvens por meio de metaescalonamento, 2012.** Tese (Doutorado em Ciência da Computação). Disponível em: <http://www.teses.usp.br/teses/disponiveis/55/55134/tde-05092012-163202/publico/Maycondefesa.pdf>. Acesso em: 10 ago. 2016.

PIEDRAHITA, Andrés Felipe Murillo. **Ferramenta de Avaliação de Ataques de Negação de Serviço em uma Plataforma de Testes**. Rio de Janeiro, 2014. Disponível em: <http://www.gta.ufrj.br/ftp/gta/TechReports/Andres14.pdf>. Acesso em: 26 maio 2016.

PONTEVES, Karine. **Fortinet:** Les multiples facettes des attaques DDoS. Disponível em: <https://www.globalsecuritymag.fr/Karine-de-Ponteves-Fortinet-Les,20130130,35135.html>. Acesso em: 22 maio 2016.

RAMOS, A et al. **Security officer:** guia oficial para formação de gestores em segurança da informação. 2° ed. Porto Alegre: Zouk, 2008.

RAY, A. K; ACHARYA. T**. Information Technology:** Principles and Applications. Prentice-Hall of India, 2004.
RIOREY. **Taxonomy of DDoS Attacks, 2015.** Disponível em: <https://static1.squarespace.com/static/5548bab5e4b08ecb6652391c/t/554923d6e4b03d6d83ac7c5e/1430856662717/RioRey_Taxonomy_DDoS_Attacks_2.6_2015-1.pdf>. Acesso em: 2 dez. 2016.

ROUSE, Margaret. **Definition:** Network Time Protocol (NTP), 2007a. Disponível em: <http://searchnetworking.techtarget.com/definition/Network-Time-Protocol>. Acesso em: 25 set. 2016.

_____. **Virtual Private Server (VPS) or Virtual Dedicated Server (VDS), 2007c.** Disponível em: <http://searchservervirtualization.techtarget.com/definition/virtual-private-server>. Acesso em: 20 ago. 2016.

_____. **Definition:** Coordinated Universal Time (UTC), 2008. Disponível em: <http://whatis.techtarget.com/definition/Coordinated-Universal-Time-UTC-GMT-CUT>. Acesso em: 26 set. 2016.

_____. **Definition:** Data as a Service, 2012. Disponível em: <http://searchcloudapplications.techtarget.com/definition/data-as-a-service>. Acesso em: 12 ago. 2016.

_____. **Definition:** firewall, 2014. Disponível em: <http://searchsecurity.techtarget.com/definition/firewall>. Acesso em: 4 abr. 2016.

_____. **Definition:** Platform as a Service (PaaS), 2015. Disponível em: <http://searchcloudcomputing.techtarget.com/definition/Platform-as-a-Service-PaaS>. Acesso em: 10 ago. 2016.

LIMA, Roni. **Support Supervisor & DoS Specialist at Maxihost:** Grupo Host. São Paulo, 2016. Disponível em: <https://br.linkedin.com/in/roni-lima-7687a3b2>. Acesso em: 20 maio 2016.

SAUTER, Molly. **The Coming Swarm:** DdoS actions, hacktivism, and civil disobedience on the Internet. Londres: Bloomsbury Publishing Plc, 2014.

SANFILIPPO, Salvatore. **Hping Documentation, 2006.** Disponível em: <http://www.hping.org/documentation.php>. Acesso em: 20 out. 2016.

SCHLEMER, Elgio. **Iptables Protege Contra SYN Flood, 2007.** Disponível em: <https://www.vivaolinux.com.br/artigo/Iptables-protege-contra-SYN-FLOOD>. Acesso em: 20 ago. 2016.

SÊMOLA, Marcos. **Gestão da segurança da informação:** uma visão executiva. 2. ed. Rio de Janeiro: Elsevier, 2014.

SEIBOLD, Michael; KEMPER, Alfons. **Database as a Service, 2012.** Disponível em: <http://goo.gl/CMQDQS>. Acesso em: 12 ago. 2016.

SILVA, Carlos Alberto. **O Elo Mais Fraco da Segurança da Informação:** pessoas representam o maior desafio. Minas Gerais: Amazon Brasil, 2015.

SOUSA NETO, Manoel Veras de. **Virtualização:** tecnologia central do datacenter. 2. edição. São Paulo: BRASPORT, 2016.

SOUZA, Lindeberg Barros de. **Projetos e implementação de redes:** fundamentos, soluções, arquiteturas e planejamento. São Paulo: Érica, 2007, 320p.

STALLINGS, William. **Criptografia e segurança de redes.** 4. ed. São Paulo: Pearson Prentice Hall, 2008.

STAIMER, Marc. **The Cloud Storage Infrastructure Decision:** public vs private, 2016. Disponível em: <http://searchcloudstorage.techtarget.com/tip/The-cloud-storage-infrastructure-decision-Public-vs-private>. Acesso em: 6 ago 2016.

TANNENBAUM, Andrew S; WETHERALL, David. **Redes de Computadores**. 5. ed. São Paulo: Pearson Prentice Hall, 2011.

TEAM Cymru, Inc. **DDoS Basics**. Disponível em: <https://www.team-cymru.com/ReadingRoom/Whitepapers/2010/ddos-basics.pdf>. Acesso em: 24 maio 2016.

TURBAN, Efraim; VOLONINO, Linda. **Tecnologia da informação para gestão:** em busca do melhor desempenho estratégico e operacional. 8°. ed. Porto Alegre: Bookman, 2013.

TUTORIALSPOINT. **Community Cloud.** Disponível em: <http://www.tutorialspoint.com/cloud_computing/cloud_computing_community_cloud_model.htm>. Acesso em: 8 ago de 2016.

VERAS, Manoel. **Arquitetura de Nuvem:** AMAZON WEB SERVICES (AWS). Rio de Janeiro: Brasport, 2013.

WIKIPEDIA. **Manifestações contra o encontro da OMC em Seattle.** 2014. Disponível em: <https://pt.wikipedia.org/wiki/Manifesta%C3%A7%C3%B5es_contra_o_encontro_da_OMC_em_Seattle>. Acesso em: 27 maio 2016.

VERISIGN. **Apresentação de Tendências de DDoS.** 2015. Disponível em: <https://www.verisign.com/pt_BR/security-services/ddos-protection/ddos-report/index.xhtml>. Acesso em: 20 jun. 2016.

ZARDIN. Eduardo de Souza**. Análise de Tráfego de Dados em Redes Locais:** estudo de caso. 2016.

ZELTSER, Lenny. **8 Reasons for Denial-of-Service (DoS)**. Disponível em: <https://zeltser.com/reasons-for-denial-of-service-attacks/#>. Acesso em: 27 maio 2016.

APÊNDICE (S)

APÊNDICE A - OFÍCIO DE SOLICITAÇÃO AO POLO UAB DE CRICIÚMA

Ofício de solicitação

Ofício n° 0001/2016 / SC

A sua Excelência o Senhor
Coordenador Júlio César Viana
Polo UAB – Criciúma
0001 – Criciúma - SC

Assunto: **Autorização do uso dos laboratórios de informática**

Eu, **HARILTON RICARDO DE SOUSA DIAS,** angolano, solteiro, inscrito no CPF sob o n° 011.778.929-10, residente e domiciliado no apartamento sito a rua Henrique Lage 730, edifício Cap Ferrat apto° 1202, bairro centro, CEP 88801-010, cidade de Criciúma, estado de Santa Catarina, acadêmico do Curso de Ciência da Computação, Universidade do Extremo Sul Catarinense, sirvo-me do presente para solicitar a Vossa Excelência **a autorização de uso dos laboratórios de informática** com a finalidade de implementar os testes práticos do meu Trabalho de Conclusão de Curso (TCC), no período de 10 de julho à 15 de dezembro.

Declaro-me ainda responsável pela reparação de qualquer dano que por ventura possa ocorrer no laboratório de informática do Polo UAB no período que eu utilizar conforme solicitação.

Limitado ao exposto, fique com os meus votos de estima e consideração.

Criciúma, 10 de julho de 2016.

Hariltom R. de Sousa Dias

Fonte: Do autor (2016).

APÊNDICE B - OFÍCIO DE SOLICITAÇÃO À *MAXIHOST*

Ofício de solicitação

Ofício n° 0002/2016 / SC

A sua Excelência o Senhor
Diretor Executivo Guilherme Soubihe Alberto
MaxiHost – São Paulo

Assunto: **Autorização para consultar a equipe técnica da Maxihost**

Eu, **HARILTON RICARDO DE SOUSA DIAS,** angolano, solteiro, inscrito no CPF sob o n° 011.778.929-10, residente e domiciliado no apartamento sito a rua Henrique Lage 730, edifício Cap Ferrat apto° 1202, bairro centro, CEP 88801-010, cidade de Criciúma, estado de Santa Catarina, acadêmico do Curso de Ciência da Computação, Universidade do Extremo Sul Catarinense - UNESC, sirvo-me do presente para solicitar a Vossa Excelência **a autorização para realizar consultas com a equipe da Maxihost a respeito do ambiente de monitoramento e proteção,** com a finalidade de aplicar a tecnologia de proteção da Maxihost no meu Trabalho de Conclusão de Curso (TCC).

Solicito também a autorização e divulgação de algumas ferramentas que fazem parte do ambiente de monitoramento e proteção, o nome da empresa e os resultados obtidos deste estudo de Conclusão de Curso (TCC).

Limitado ao exposto, fique com os meus votos de estima e consideração.

Criciúma, 20 de setembro de 2016.

Hariltom R. de Sousa Dias

Fonte: Do autor (2016).

APÊNDICE C - ARTIGO

Segurança de Sistemas Computacionais: Avaliação de uma Contramedida Contra-Ataques de Negação de Serviço Baseada na *Cloud Computing*

Harilton Ricardo de Sousa Dias[1], Paulo João Martins[2]

[1]Curso de Ciência da Computação – Universidade do Extremo Sul Catarinense (UNESC) – Criciúma, SC – Brasil

[2]Curso de Ciência da Computação – Universidade do Extremo Sul Catarinense (UNESC) – Criciúma, SC – Brasil

harilton-dias@hotmail.com, pjm@unesc.net

Abstract. *Denial of Service (DoS) attacks represent one of these threats. This type of threat directly affects the Quality of Service (QoS) and the amount of available resources on a network, preventing their legitimate users from accessing and performing their activities. The study of this research, consisted of the evaluation of a mitigation countermeasure based on cloud computing and its service models. For its conception, the following methodology was used: bibliographic research, and the elaboration of a case study where four (4) steps were applied, namely: authorization of the entities involved, preparation of the application scenario, reading and extraction of data, and documentation of results obtained. Data were obtained from two monitoring panels provided by the company involved in the study. The results help security professionals understand and deal with the risks of DoS attacks, yon reduce the burden on analysts and network administrators. With this post, it is understood that the present research successfully achieved its purpose.*

Resumo. *Ataques de Negação de Serviço (Denial of Service - DoS) representam uma destas ameaças. Este tipo de ameaça afeta diretamente a qualidade de serviço (Quality of Service - QoS) e a quantidade de recursos disponíveis em uma rede, impedindo que seus usuários legítimos tenham acesso e realizam suas atividades. O estudo desta pesquisa, consistiu na avaliação de uma contramedida de mitigação contra-ataques DoS baseada na cloud computing e nos seus modelos de serviço. Para a sua concepção, seguiu-se a seguinte metodologia: pesquisa bibliográfica, e a elaboração de um estudo de caso onde aplicou-se quatro (4) etapas, nomeadamente: autorização das entidades envolvidas, preparação do cenário de aplicação, leitura e extração dos dados, e documentação dos resultados obtidos. Os dados foram obtidos a partir de dois painéis de monitoramento fornecidos pela empresa envolvida no estudo. Os resultados auxiliam os profissionais de segurança a entender e a lidar com os riscos de ataques DoS, além de reduzirem a carga sob analistas e administradores de redes. Com isto posto, subentende-se que a presente pesquisa alcançou com sucesso o seu propósito.*

1. Introdução

Existe um consenso na nossa sociedade de que o bem mais valioso do século XXI é a informação. Os últimos anos foram marcados pela propagação progressiva de equipamentos de comunicação, deixado de ser o computador o único meio tecnológico e digital do nosso dia a dia, percorrendo por outros tipos de dispositivos, particularmente os dispositivos móveis como *smartphones*, *tablets*, *smartwatches*, assistentes virtuais, entre outros. Consequentemente, existe uma grande disseminação de informações estratégicas e de grande importância que circulam na maior infraestrutura de rede pública de comunicação, à Internet (CARISSIMI; ROCHOL; GRANVILLE, 2009).

Com todas estas informações a circular em uma infraestrutura de rede pública, estende-se há necessidade de garantir a proteção destes ativos frente as inúmeras ameaças a que estão sujeitos. Worms, vírus, engenharia social, malwares, keyloggers, entre outras ameaças, representam o cenário a que estamos expostos. Contudo, esta pesquisa centraliza o seu estudo nos ataques de Negação de Serviço (Denial of Service - DoS) e na sua variável distribuída, os ataques Distribuídos de Negação de Serviço (Distributed Denial of Service - DDoS). Os seus intentos, visam esgotar todos os recursos disponíveis em um servidor através da produção de tráfego malicioso, que resulta na queda parcial ou total de um servidor.

A implementação de um modelo avançado e de estratégias de gestão, proteção e monitoramento de tráfego de rede em tempo real, garantem uma maior produtividade, um maior desempenho e qualidade na entrega de serviços e ferramentas aos usuários legítimos da rede.

No decorrer dos anos, vários serviços e ferramentas para combater ataques de negação de serviço foram desenvolvidas. Esta pesquisa visa explorar uma solução inovadora de proteção baseada na cloud computing, que propõe o estudo de um caso onde é realizado um ataque DoS controlado, e a aplicação de uma contramedida de mitigação baseada na cloud computing.

2. Sistemas de Informação

Há muito, as empresas têm sido influenciadas por transformações e inovações que surgem no mercado, onde nos últimos anos registram e vivenciam a velocidade da evolução na era da informação20. No mundo moderno as organizações não só devem se preocupar com a competição global, mas também em como manter protegido o seu ativo mais valioso, a informação (SÊMOLA, 2014).

Para perceber como os sistemas de informação são importantes, pode-se analisar o estudo conduzido por Laudon e Laudon (2014), onde retrata a notável e enorme valorização que o mundo do esporte obteve nas últimas décadas, que embora esporte, é uma das atividades humanas mais praticadas e vistas. Trata-se do estádio do *New York Yankees*. No estudo, os autores descrevem os desafios que os engenheiros tiveram para criar o estádio mais cabeado, conectado e com disposição para vídeo, oferecendo mais espaço e conforto. Para que tudo isso fosse possível, a solução foi à aplicação de sistemas de informação.

2.1. Segurança da Informação

No contexto da norma, a segurança da informação é a proteção contra vários tipos de ameaças para assegurar a continuidade do negócio, reduzir o risco, potencializar o retorno sobre os investimentos e as oportunidades do negócio, ou seja, preservar a confidencialidade, integridade, e disponibilidade da informação; ampliando as demais propriedades, autenticidade, responsabilidade, não repúdio e confiabilidade (NBR ISO/IEC 27002, 2013).

[20] Dados que passam por algum tipo de processamento para que possam ser utilizados de maneira inteligível (DANTAS, 2011).

Seguindo os padrões internacionais, a segurança da informação precisa sempre atender os seus três elementos básicos (RAMOS, 2008):

a) **confidencialidade:** uma informação só pode ser acessada por quem possui um determinado nível de privilégio ou autorização, ou seja, basicamente, estamos falando de sigilo;
b) **integridade:** implica no facto de que uma informação só deva ser modificada por quem tem a devida autorização. Estas modificações podem ser tanto intencionais quanto acidentais;
c) **disponibilidade:** uma informação deve estar sempre disponível para quem for autorizado e necessitar consultá-la. Esta informação ou o meio informático (sistema, servidores, entre outros) deve estar disponível 24h por dia, 7 dias por semana.

3. Segurança em Redes de Computadores

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), que é mantido pelo Comitê Gestor da Internet no Brasil (NIC.br), tem sido uma central de notificações de incidentes de segurança no Brasil. O Cert estabelece diretrizes estratégicas, promove estudos entre outras atribuições e objetivos (CERT.br, 2012).

A figura 1 demonstra um desses estudos, registrando o total de incidentes ocorridos por ano, desde 1999 a 2015 (CERT.br, 2016).

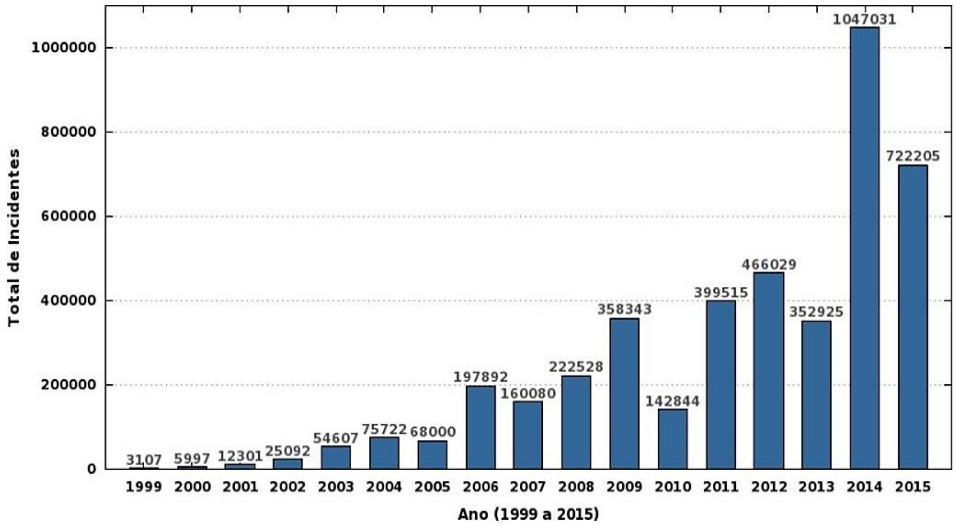


Figura 1. Total de incidentes reportados ao Cert.br por ano

O estudo conduzido pela *Nexusguard*, empresa líder global em soluções de segurança, complementa ao apontar que no seu primeiro trimestre de estudo, o Brasil foi o terceiro maior alvo de ataques DoS/DDoS do mundo, e o primeiro da América Latina. Ao todo, foram avaliados 180 países, Estados Unidos e China ocuparam as primeiras posições (Nexusguard, 2016, traduçã nossa).

4. Ataques de Negação de Serviço

Negação de Serviço, do inglês Denial of Service (DoS) é uma técnica que consiste em retirar de operação um serviço, um computador, ou uma rede conectada à Internet. Normalmente, o atacante utiliza um equipamento que já esteja conectado a esta rede. É o que diz o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br, 2016).

Ataques de negação de serviço representam atualmente uma séria ameaça para o correto funcionamento da Internet, e nos últimos anos, o tráfego malicioso gerado por esses ataques só vem se multiplicando. Os mecanismos de defesa tradicionais para ataques de negação de serviço seguem uma abordagem reativa, ou seja, só depois que os ataques desse tipo causam enormes prejuízos é que se procura novos mecanismos de defesa que estejam à altura. Esta abordagem não é aceitável levando em consideração o grau de risco que esses tipos de ataque representam (PIEDRAHITA, 2014).

Quando utilizado de maneira coordenada e distribuída, ou seja, quando um conjunto de equipamentos é utilizado para a realização do ataque, recebe o nome de Ataque Distribuído de Negação de Serviço, do inglês, Distributed Denial of Service (DDoS) (CERT.br, 2016).

4.1 Causas de Ataques de Negação de Serviço

Ataques DoS acontecem devido as restrições que as infraestruturas possuem, ou seja, algumas vulnerabilidades não podem ser resolvidas devido ao limite de largura de banda, ou de conexões ativas comum a todos os dispositivos de uma rede, sejam eles físicos ou de software. Por exemplo, se um servidor web possui uma capacidade de aceitar mil pedidos por segundo, então o milésimo primeiro pedido será negado. É comum para as organizações ao ultrapassar a capacidade do seu servidor, realizar atualizações ou até mesmo trocar por outro software que aceite mais pedidos. Todavia, a plataforma atual de hardware pode não suportar esse novo software, exigindo assim upgrades de CPU e de memórias RAM (BASTA, 2014).

4.2 Tipos de Ataques DoS

Basicamente existem cinco tipos de ataques de negação de serviço: (1) ataques evitáveis, (2) não evitáveis, (3) ataques baseados em software por inundação, (4) ataques isolados e (5) distribuídos (BASTA, 2014):

a) **DoS evitável:** ocorrem quando o sistema é projetado pelo administrador de redes para executar vários serviços sem ter em conta a sua limitação, seja em nível de rede ou de aplicação. Por exemplo, o administrador projeta um sistema baseado em VoIP (voz sobre IP) com 120 telefones, estimando em média um uso de 20% do tempo, sem medir a capacidade de uso, dessa forma, admite que a capacidade do sistema seja suficiente somente para acomodar um em cada cinco usuários a cada momento. Isso funciona bem tanto na teoria como na prática, até que, seja convocada uma audioconferência e mais de 30% dos funcionários da empresa participem. Como o sistema foi projetado com apenas 20% de uso, ao exceder esse limite o sistema vai falhar: as chamadas serão derrubadas e haverá várias ordens de serviço de manutenção. A esta perda de recursos disponíveis resulta a um tipo de DoS;

b) **DoS não evitável:** já sugestivo e diferente do primeiro, o administrador não pode o evitar que aconteça, visto que o administrador do sistema não pode o prever, portanto, não está preparado. Por exemplo, o administrador recebe um aviso que uma das impressoras não está a funcionar e ao se conectar ao servidor, verifica que há uma grande quantidade de trabalhos em fila e que não podem ser impressos por estarem mal formatados. Eles consomem todo o espaço disponível em disco, negando assim o acesso a outros usuários. Nesse caso, é bem provável que esteja a acontecer um ataque ao servidor de impressão, resultando em uma negação de serviço;

c) **ataques por inundação:** de maneira geral, processos em execução, seja em computadores ou dispositivos de rede, demandam de largura de banda e espaço de memória e em disco. Também necessitam de estruturas de dados e tempo de CPU o seu correto funcionamento. Sendo que os dispositivos vêm de fábrica programados com uma

capacidade máxima de processamento de pacotes. Ataques de inundação consomem esses recursos limitados, sobrecarregando assim a rede e negando recursos a usuários legítimos;

d) **ataques isolados:** provém de uma única fonte e podem ser facilmente bloqueados a partir de um firewall;

e) **ataques distribuídos:** este tipo de ataque é gerado por várias fontes simultaneamente. Ataques DDoS são mais difíceis de serem bloqueados com listas de controle de acesso (ACL) ou regras de firewall.

De acordo a taxonomia de ataques DoS/DDoS classificada por Riorey (2015, tradução nossa), os ataques de inundação de pacotes podem ser:

a) ***SYN Flood*** (baseado no protocolo TCP): neste tipo de ataque, o servidor vítima recebe centenas e centenas de requisições de abertura de conexão SYN, o atacante pode falsificar os endereços de IPs para dificultar o bloqueio do ataque;

b) ***SYN-ACK-Flood*** (baseado no protocolo TCP): o servidor vítima passa a receber centenas e centenas de requisições de abertura de conexão SYN-ACK a partir de endereços falsificados;

c) ***ACK & Push ACK Flood*** (baseado no protocolo TCP): o servidor vítima passa a receber centenas e centenas de pacotes do tipo ACK falsificados, onde a taxa de envio pertence a uma qualquer outra sessão legítima dentro da lista de conexão ao servidor;

d) ***Fragmented ACK*** (baseado no protocolo TCP): este tipo de ataque consiste em consumir a maior quantidade de banda possível, é possível definir para cada pacote até 1500 bytes;

e) ***RST ou FIN FLOOD*** (baseado no protocolo TCP): um servidor vítima passa a receber centenas e centenas de pacotes do tipo RST ou FIN falsificados, onde a taxa de envio não pertence a qualquer outra sessão legítima dentro da lista de conexão do servidor;

f) ***Synonymous IP*** (baseado no protocolo TCP): são enviados pacotes do tipo TCP-SYN falsificados em uma taxa elevada para o servidor vítima, estes pacotes contém a informação do servidor descrita como: endereço de IP de origem e de destino;

g) ***UDP Flood*** (baseado no protocolo UDP): são enviados milhares de pacotes falsificados do tipo UDP a partir de centenas de fontes de Ips de origem, normalmente neste tipo de ataque, as taxas de envio são muito altas;

h) ***UDP Fragmentation*** (baseado no protocolo UDP): é uma variante do ataque do tipo *UDP Flood*, contudo, o servidor vítima pode receber uma variação alta ou baixa de pacotes num tamanho de até 1500 bytes;

i) ***DNS Flood*** (baseado no protocolo UDP): são utilizadas diversas fontes de origem para falsificar pacotes DNS a taxas altas, todavia, o servidor vítima entende que são requisções válidas;

j) ***VoIP Flood*** (baseado no protocolo UDP): o servidor vítima recebe centenas e centenas de pacotes do tipo VoIP, que são originados a partir de diversas fontes de origem e com taxas altas;

k) ***Media Data Flood*** (baseado no protocolo UDP): outra variante do *UDP Flood*, no entanto, neste tipo de ataque os pacotes apresentam como tipo de ficheiro dados de mídea;

l) ***Non-Spoofed UDP Flood*** (baseado no protocolo UDP): nesta variante, os pacotes não são falsificados e são enviados em taxas altas;

m) ***ICMP Flood*** (baseado no protocolo ICMP): são enviados diversos pacotes falsificados ICMP, de diferentes fontes de origem e com taxas altas para o servidor vítima;

n) ***ICMP Fragmentation*** (baseado no protocolo ICMP): variante do *ICMP Flood*, o servidor vítima recebe pacotes fragmentados com tamanho de 1500 bytes e que não podem ser remontados;

o) ***Ping Flood*** (baseado no protocolo ICMP): são enviados para o servidor vítima ICMP echo requests (ping), originados a partir de diversas fontes e com taxas altas.

4.3 Métodos de Prevenção Contra-Ataques DoS

Pascucci (2013, tradução nossa), especialista e pesquisador em segurança da informação, sugere três técnicas para prevenção de ataques DoS:

1ª **sugestão:** determinar os recursos existentes e avaliá-los de modo a saber se podem limitar ou reduzir alguns ataques. Por exemplo, limitações de tráfego em firewall ou em load balancers, criação de procedimentos para contatar o ISP, realização de bloqueios geográficos de IP, configuração de alertas de aumento de tráfego, condições de cortar ou remover algum serviço que atue na da camada de aplicação e a implementação de um processo de resposta a incidentes de ataques DoS;

2ª **sugestão:** implementação de aparelhos de fornecedores como a *Arbor Networks, Fortinet, Check Point*, entre outros, que ajudam a prevenir ataques de negação. No entanto, o especialista destaca que apesar de serem aparelhos sofisticados, são aparelhos caros ou com assinaturas altas, e exigem treinamentos constantes;

3ª **sugestão**: o autor sublinha esta última sugestão como sendo a com maior potencial e capacidade para absorver ataques DoS. A solução consiste no uso de uma rede de distribuição de conteúdo (CDN) para filtrar o tráfego malicioso antes mesmo de chegar aos servidores locais.

De acordo ao Cert (2016), a segurança de uma rede depende proporcionalmente da segurança dos demais setores que formam à Internet. Desta forma, recomenda quatro ações que devem ser tomadas de modo a reduzir a incidência de ataques DoS:

a) **usuários finais:** precisam ter bastante atenção para não serem voluntareamente utilizados remotamente como robõs para ampliarem ataques DoS. O uso de técnicas como a engenharia social, levam usuários a pensarem que estão a contribuir com alguma causa, quando na verdade estão a ser enganados ao permitirem acesso às suas máquinas para cibercriminosos. Normalmente, estes usuários são atraídos por meio da instalação de ferramentas ou por portais especifícos. Uma política adequada de segurança e programas de conscientização, ajudam os usuários a estar a par das ameaças existentes e das medidas que podem ser tomadas;

b) **desenvolvedores de aplicações Web:** junto com os links de comunicação, fazem parte dos princípais alvos dos ataques DoS, isto porque possuem capacidades muito altas de processamento, banda e armazenamento (ambientes bem estruturados). Para os atacantes, são os ambientes perfeitos para instalarem suas ferramentas DoS;

c) **administradores de redes:** podem melhorar o cenário de ataques DoS e de ameaças em geral, seguindo e implementando à risca as boas práticas de segurança. Devem ainda adotar uma abordagem proativa para algumas situações. Recomenda-se também, a participarem voluntareamente ao notificarem sobre incidentes ocorridos aos orgãos responsáveis pelos estudos e tratamentos de incidentes (Cert, Nic, entre outros). Outras boas práticas como: (1ª) atualizar os equipamentos e serviços (SGDB, módulos e plugins), (2ª) configurar corretamente serviços e aplicações, (3ª) monitorar logs, (4ª) monitorar todo tráfego de entrada e saída, (5ª) ser criterioso, (6ª) controle de permissões e privilégios

de usuários, (7ª) elaboração de políticas de segurança adequadas, (8ª) campanhas de sensibilização, (9ª) possuir funcionários qualificados, e (10ª) acompanhar as tendências de ataques e vulnerabilidades, bem como, novas soluções de segurança, permitem reduzir o número de incidentes e a fortalecer a estrutura de segurança do ambiente;

d) **provedores de conectividade:** da mesma forma, devem seguir as boas práticas de segurança, visto que ao implementá-las fortalecem não só à sua infraestrutura, mas como também a de seus clientes. Algumas práticas como: (1) habilitar o filtro *antispoofing*, (2) proteger os CPEs dos clientes, (3) e configurar adequadamente os serviços, principalmente os com base nos protocolos DNS, NTP, SNMP, SSDP, UDP, TCP/IP auxilam na prevenção de ataques DoS.

5. *Cloud Computing*

A Computação em Nuvem, do inglês Cloud Computing, está sendo responsável por uma das maiores revoluções nos últimos anos na área de Tecnologia da Informação (TI) (OPUS SOFTWARE, 2015).

A cloud computing é um novo modelo de negócio que cada vez mais cresce e ganha espaço no mercado de TI, seu modelo garante a entrega de diferentes serviços, dos quais, a segurança foi o foco deste trabalho. *Intrusion Detection System* (IDS), *Intrusion Prevention System* (IPS) e *Content Delivery Network* (CDN), são mecanismos eficazes para detecção e prevenção de ataques de negação de serviço (ALQAHTANI; BALUSHI; JOHN, 2014, tradução nossa).

5.1 Contramedida de Mitigação Contra-Ataques DoS baseada na *Cloud Computing*

Em um mercado competitivo, as organizações precisam avaliar ferramentas e serviços que ofereçam soluções de segurança, sejam estas locais ou em *cloud*. Devem avaliar também quais soluções melhor atendem os requisitos da sua rede considerando as possíveis ameaças que estão expostas, sejam elas internas ou externas (PEREIRA; DANTAS; MEDEIROS, 2012).

Empresas como *Maxihost*, *CloudFlare*, *Incapsula*, *Akamai Tecnologies*, *Verisign*, *Nexusguard*, entre outras, já oferecem o serviço de filtrar todo tráfego malicioso através de suas próprias redes antes que ele atinja seus clientes (PASCUCCI, 2013, tradução nossa).

5.1.1 *Monitoramento, Detecção e Mitigação Maxihost*

Umas das tecnologias utilizadas pela Maxihost para monitorar, detectar e mitigar ataques DoS sem afetar o cloud server, são os equipamentos da NsFocus, empresa líder na distribuição exclusiva de proteção contra-ataques DoS (LIMA, 2016).

O sistema de proteção *Anti-DoS-System* (ADS) possui uma arquitetura escalável, o que na prática garante uma performance otimizada. O Sistema está composto por três componentes (NSFOCUS, 2016, tradução nossa):

a) ***Network Traffic Analyzer* (NTA):** tem a função de detectar ameaças e identificar o tráfego malicioso;

b) ***Anti-DoS System* (ADS):** permiti mitigar todo o tráfego malicioso, ou seja, o tráfego indesejado;

c) ***Anti-DoS System Manager* (ADS-M):** é uma ferramenta de gestão centralizada que permite o controle e suporte dos usuários, e os módulos NTA e ADS.

Para detectar e separar tráfego malicioso de uma rede, os equipamentos efetuam uma análise e inspeção severa a partir de um motor multiestágio do sistema Anti-DoS System (ADS). A ação garante que todos os protocolos sejam submetidos a uma série de algoritmos de análise e inspeção (NSFOCUS, 2016, tradução nossa).

Outros mecanismos são também utilizados para garantir a detecção do tráfego malicioso (NSFOCUS, 2016, tradução nossa):

a) verificações a partir de comandos (RFC);

b) análise de protocolos e aplicações;

c) lista de controle de acesso;

d) reputação do IP (blacklists, entre outros);

e) anti-spoofing;

f) análise algorítmica nas camadas 3 e 4 do modelo OSI.

6. Estudo de um Caso de Ataque de Negação de Serviço, Utilizando uma Contramedida de Mitigação Baseada na *Cloud Computing*

Os serviços da *cloud* pública ou redes de computadores não estão imunes as várias ameaças de segurança existentes, e uma boa parte destas ameaças envolvem ataques de negação de serviço. Cibercriminosos não se limitam apenas ao roubo de dados, eles podem ocasionar falhas nas aplicações com solicitações de tráfego malicioso. A ferramenta mais comum contra este tráfego indesejado tem sido o *firewall* tradicional. No entanto, o gerenciamento de um *firewall* tende a ser problemático e demorado, especialmente para ataques DDoS, o volume de tráfego gerado é sempre muito alto, é o que explica *Stephen Bigelow*, editor de tecnologia sênior com mais de 20 anos de experiência e com certificação *CompTIA* em segurança de redes de computadores e servidores (BIGELOW, 2016, tradução nossa).

Esta pesquisa teve como finalidade avaliar o comportamento de um ataque DoS SYN Flood, e da contramedida de mitigação fornecida pela Maxihost[21]. Um ataque DoS, é caracterizado principalmente por violar umas das propriedades básicas da segurança, que é a disponibilidade.

6.1 Metodologia

Para materialização deste trabalho de conclusão de curso, procedeu-se a um levantamento bibliográfico específico, focado no tema de defesa, seguido de uma análise e síntese para identificação da matéria pertinente e imprescindível à sua concepção. Parte das obras disponibilizadas são de origem anglófona, e integram artigos científicos e dissertações para títulos de bacharel e mestre, encontrando-se hospedadas em repositórios científicos como o Repositório Científico de Acesso Aberto de Portugal, os Periódicos CAPES, a biblioteca digital ieexplore e Jornais Científicos, entre outros. No decorrer da pesquisa, fez-se necessário deslocar à Maxihost para consolidar a parceria e obter informações complementares.

[21] Fundada em 2001, a empresa atua no mercado há mais de quinze anos, e é provedora de soluções de servidores cloud e dedicado que mais cresce no Brasil. A Maxihost oferece serviços de cloud computing, hosting dedicado, colocation e serviços de gerenciamento (backup e storage, monitoramento e proteção DoS). A sua tecnologia de proteção contra-ataques DoS e DDoS é exclusica e pioneira no Braisl.

6.2 Cenário de Aplicação

Para elucidação e contextualização do estudo, foram consideradas as seguintes situações (figura 2):

a) **a primeira situação é representada por um cenário de ataque:** onde um indivíduo realiza um ataque DoS, e tenta sobrecarregar à rede com mais requisições de acesso do que àquelas que um servidor suportaria;
b) **a segunda situação é representada por um cenário de vítima:** onde um usuário legítimo desta rede, que realiza as suas atividades rotineiras, (acesso a sites acadêmicos e a sites corporativos, entre outras atividades) deixa de obter respostas do servidor por ser vítima de um crime digital;
c) **a terceira e última situação é representada por um cenário de defesa:** onde apresenta-se a abordagem de defesa e mitigação contra-ataques DoS da Maxihost.

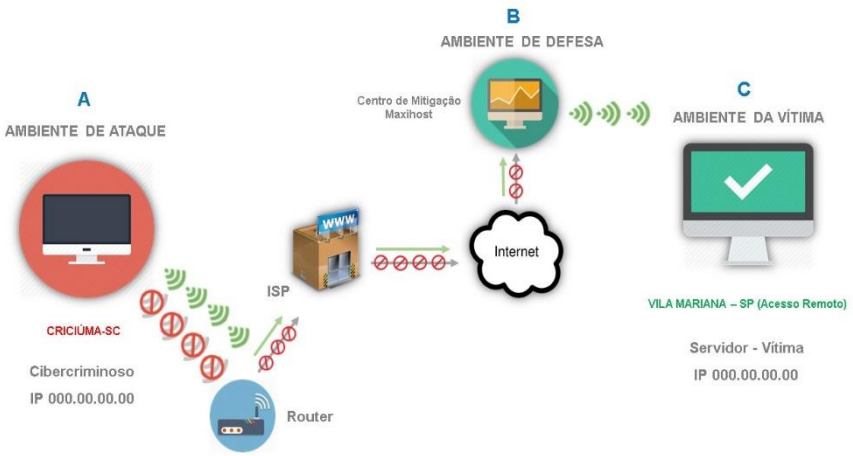


Figura 2. Cenário de Aplicação: ataque, defesa e vítima

6.3 Autorização

O trabalho foi realizado em um dos polos da Universidade Aberta do Brasil (UAB), localizado em Criciúma/SC, e pela empresa Maxihost (via acesso remoto), localizada na Vila Mariana/SP. Foi solicitado por escrito um ofício ao coordenador Polo UAB de Criciúma, a fim de obter a devida autorização para realização do estudo de caso. Seguidamente, foi recebida a resposta. Solicitou-se também por escrito outro ofício à Maxihost, a fim de demonstrar e consultar a aquipe técnica da empresa.

6.4 Preparação

Para controle e execução do ataque DoS foram estabelecidas algumas diretrizes: (1ª) o período matunino e/ou vespertino para execução do ataque, (2ª) um tempo máximo de ataque de até 1h, (3ª) a geraração do tráfego malicioso, (4ª) o SYN *Flood* como tipo de ataque, e (5) a leitura e extração dos resultados dos testes referentes ao mês de outubro.

A primeira etapa consistiu em simular o comportamento de um usuário legítimo da rede, acessou-se remotamente o servidor vítima onde foram acessadas algumas páginas e o download de alguns arquivos. O pico máximo de tráfego legítimo foi de 13 Mbps, uma vez que os valores foram suficientes para obter os resultados da pesquisa, não houve a necessidade de ampliar tanto o tráfego legítimo quanto ao volume de tráfego malicioso. A figura 3 mostra um gráfico de área que desta os picos máximo de tráfego legítimo da rede em uma média de 30 segundos numa relação “bits per second x tempo”.

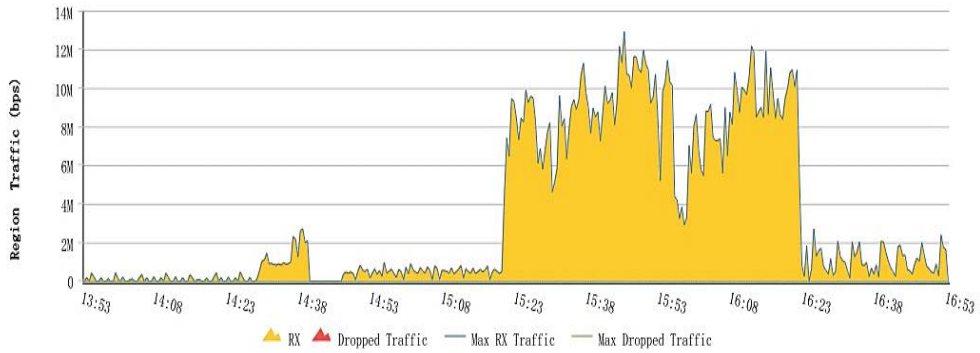


Figura 3. Tráfego legítimo

A segunda etapa, e com o auxílio do software hping, foi originado o ataque enviando milhares de pacotes falsificados do tipo SYN, definidos com o tamanho máximo de 1400 databytes (tabela 1).

Tabela 1. Comando e log de execução do ataque SYN Flood

```
root@servidordeataque:~# hping3 -d 1400 -S -w 64 -p 80 --flood 189.x.x.x
HPING 189.x.x.x (eth0 189.x.x.x): S set, 40 headers + 1400 data bytes
hping in flood mode, no replies will be shown

--- 189.x.x.x hping statistic ---
28471601 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@servidordeataque:~#
```

6.5 Leitura e Extração dos Resultados Obtidos

A partir das informações extraídas dos painéis de monitoramento da *Maxihost*, observou-se que o sistema foi capaz de bloquear e encaminhar todo tráfego de ataque para o centro de mitigação num intervalo de 30 a 50 segundos. Nesta ocasião, o tráfego legítimo (marcado em amarelo) havia atingido um pico máximo de 29 Mbps. O tráfego de ataque (tráfego malicioso) atingiu 20 Mbps e teve uma duração aproximada de 17 min (figura 4).

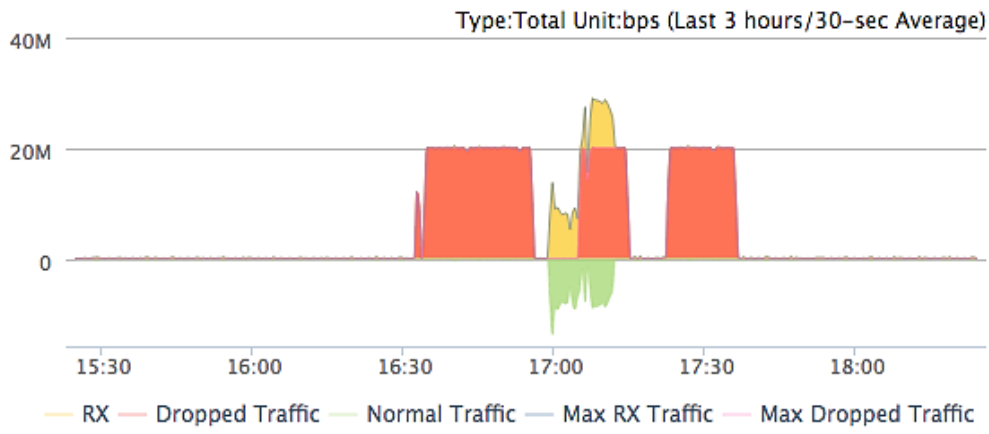


Figura 4. Bloqueio e separação do tráfego malicioso

Observou-se na figura o surgimento do tráfego malicioso (marcado a vermelho), originado do ataque de inundação SYN Flood, que teve início aproximadamente às 16h33min. Constatou-se

nas amostragens, que o protocolo TCP direcionado para as portas 80 e 21, e o protocolo UDP direcionado para as portas 23 e 161, foram os que maior incidência de ataque sofream. No total, o endereço IP de ataque apareceu 168 vezes na lista de fontes.

Para complemtar o seu sistema de defesa, à *Maxihost* possui uma *blacklist*, onde o sistema automaticamente adiciona todos endereços IPs que representam uma ameaça para de rede.

7. Conclusão

Com os dados obtidos foi possível interpretar que a execução do ataque DoS, quando não identificada, provê de uma taxa de êxito muito alta, principalmente na ausência de uma ferramenta ou serviço capaz de mitigar a ameaça. Não resta dúvidas que o uso da *cloud computing* como solução de segurança, fornece diversas vantagens como a relação custo-benefício, uma maior flexibilidade, o modelo *pey-per-use*, alta dispobilidade, entre outras.

A pesquisa realizada permitiu avaliar o comportamento de um dos tipos de ataques de inundação (SYN Flood), e de uma contramedida baseada na *cloud computing*. No decorrer desta pesquisa foram encontradas algumas dificuldades, sendo estas resolvidas posteriormente, permitindo deste modo a apresentação e aplicação da solução proposta. Umas das dificuldades encontradas, se não, a que maior grau de dificuldade apresentou, foi sobre a impossibilidade de realizar uma conexão direta com a empresa, em razão da inviabilidade e por suplantarem os limites financeiros do acadêmico. Todavia, esta situação foi contornada quando se criou a vítima dentro da própria empresa.

O sistema de proteção da Maxihost mostrou ser uma solução inovadora e com diversas características peculiares. A solução reúne recursos necessários para manter as propriedades básicas da segurança preservadas.

Concluindo, este trabalho abre portas para outras linhas de pesquisa na área de segurança de sistemas computacionais, tais como: a implantação de uma cloud privada, poderia ser feito também um estudo mais detalhado de outros métodos de ataque, outra linha de pesquisa, seria no estudo de técnicas mais eficientes que permitissem elevar a taxa de êxito ao se rastrear a origem dos ataques DoS.

8. Referências

Abnt NBR ISO/IEC 27002. “Tecnologia da Informação, Técnicas de Segurança: código de prática para gestão da segurança da informação”. Associação Brasileira de Normas Técnicas, 2013 http://www.abntcatalogo.com.br/norma.aspx?ID=306582.

Alqahtani, S. M, Balushi, Al, John, R. (2014). “An Intelligent Intrusion Prevention System for Cloud Computing (SIPSCC)”. [Artigo IEEE Xplore Digital Library]. https://goo.gl/qA88As.

Basta, A. (2014). “Glossário: bootnets, hacktivismo”. São Paulo: Cengage Learning.

Bigelow, S. J. (2016). “Create a Cloud DDoS Protection Plan”. http://searchcloudcomputing.techtarget.com/tip/Create-a-cloud-DDoS-protection-plan.

Carissimi, A. S., Rochol, J., Granville, L. Z. (2009). “Redes de Computadores”. Porto Alegre: Artmed.

Cert.br. Centro de Estudos, Resposta e Tratamento de Incidentes no Brasil. (2012). “Sobre o CERT.br”. http://www.cert.br/sobre/.

Cert.br. (2015). “Incidentes Reportados ao CERT.br: janeiro a dezembro”. http://www.cert.br/stats/incidentes.

Cert.br. (2016). “Recomendações para Melhorar o Cenário de Ataques Distribuídos de Negação de Serviço (DDoS)”. http://www.cert.br/docs/whitepapers/ddos/#5.

Cert.br. (2016b). “Sobre nós”. <http://maxihost.com.br/sobre/>.

Dantas, M. L. (2011). “Segurança da Informação: uma abordagem focada em gestão de riscos”. Pernambuco: Olinda.

Laudon, K. C, Laudon, J. P. (2011). “Sistemas de informação Gerenciais”. 11ª ed. São Paulo: Pearson Education.

Lima, R. (2014). “Support Supervisor & DoS Specialist at Maxihost: Grupo Host”. São Paulo, https://br.linkedin.com/in/roni-lima-7687a3b2.

Maxihost. (2016). Proteção DoS e DDoS. http://maxihost.com.br/protecao-ddos/.

Nsfocus. (2014). “Anti-DDoS System White Paper”. https://goo.gl/zUokCh”.

Opus, Software. (2015). “Computação em Nuvem”. 1. ed. São Paulo: OPUS Software Ltda.

Pascucci, M. (2013). “Preventing a Distributed Denial-of-Service Attack: is hardware needed”. https://goo.gl/mccjn4.

Pereira, J. P. A. (2014). “Método de Mitigação Contra Ataques de Negação de Serviço Distribuídos Utilizando Sistemas Multiagentes”. https://goo.gl/VcUszb.

Piedrahita, A. F. M. (2014). “Ferramenta de Avaliação de Ataques de Negação de Serviço em uma Plataforma de Testes”. Rio de Janeiro. http://www.gta.ufrj.br/ftp/gta/TechReports/Andres14.pdf.

Ramos, A et al. (2008). “Security officer: guia oficial para formação de gestores em segurança da informação”. 2°ed. Porto Alegre: Zouk.

Riorey. “Taxonomy of DDoS Attacks”. https://goo.gl/lbrYvR.

Sêmola, M. (2014). “Gestão da segurança da informação: uma visão executiva”. 2. ed. Rio de Janeiro: Elsevier.

ANEXO (S)

ANEXO A - RESPOSTA DE OFÍCIO DE SOLICITAÇÃO AO POLO UAB DE CRICIÚMA

POLO UAB **Criciúma**

Criciúma, 20 de setembro de 2016.

Ref: Resposta ofício n° 0001/2016 – SC

Prezado,

Em resposta ao **Ofício n° 0001/2016**, onde solicita a autorização para o uso do laboratório de informática do Polo, e se declara como responsável por qualquer dano. Informo que autorizo e apoio o seu projeto de conclusão de curso.

Atenciosamente,

COORDENAÇÃO-EàD
PÓLO DE CRICIÚMA
Universidade Federal de Santa Catarina

Júlio Cesar Viana
Coordenador

Ao Senhor
Harilton Ricardo de Sousa Dias
Acadêmico do Curso de Ciência da Computação
Universidade Extremo do Sul Catarinense – UNESC
Criciúma – Santa Catarina

Fonte: Do autor (2016).

ANEXO B - RESPOSTA DE OFÍCIO DE SOLICITAÇÃO À *MAXIHOST*

maxihost

São Paulo, 31 de outubro de 2016.

Ref: Resposta ofício n° 0002/2016 – SC

Prezado,

Em resposta ao **Ofício n° 0002/2016**, onde solicita a autorização para consultar a equipe técnica da Maxihost, e divulgar algumas das ferramentas que fazem parte do nosso ambiente de monitoramento e proteção. Informo que Maxihost autoriza e apoia o seu projeto de conclusão de curso.

Atenciosamente,

Guilherme Soubihe Alberto
Diretor Executivo

Ao Senhor
Harilton Ricardo de Sousa Dias
Acadêmico do Curso de Ciência da Computação
Universidade Extremo do Sul Catarinense – UNESC
Criciúma – Santa Catarina

Fonte: Do autor (2016).

ANEXO C - FICHA DE DADOS PROTEÇÃO PARA REDES (PFN) & PROTEÇÃO PARA SERVIÇOS (PFS) - *MAXIHOST* SERVIÇOS DE INTERNET LTDA

maxihost

Cloud DDoS Protection
(CDP)

Protection for Networks
(PFN)

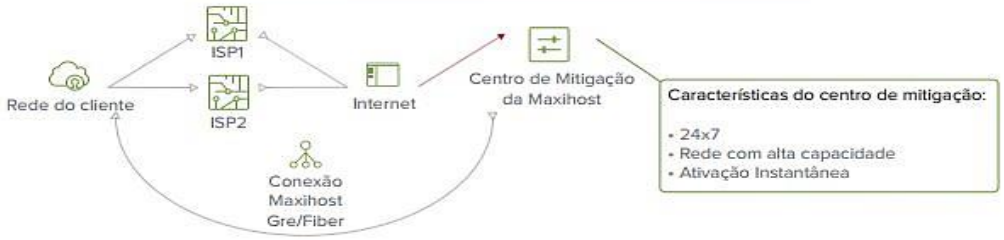
Mantenha o seu tráfego fluindo com a solução de proteção contra ataques de negação de serviço da Maxihost. Ela protege provedores de serviço e redes corporativas contra ataques do tipo DoS e DDoS. Com base em uma arquitetura de rede global, a PFN pode ser ativada em um instante para mitigar a mais ampla gama de ataques DDoS.

Benefícios da PFN

- Mitigação 24x7 com SLA garantido
- Proteção para todo o bloco de IP contra ataques
- Alta capacidade de rede e baixa latência - os ataques são mitigados em nossos centros de mitigação, distribuídos geograficamente
- Não é necessário nenhum hardware ou software adicional. Utilize apenas sua infraestrutura existente
- Solução flexível - anuncie seu tráfego de entrada para Maxihost o tempo todo ou apenas quando necessário
- Portal de usuário baseado na Web - permite o monitoramento em tempo real, através de um dashboard
- Compatível com redes em qualquer lugar do mundo
- Não adiciona ponto de falha na rede

Como funciona

1. Conecte-se à rede da Maxihost virtualmente (túnel GRE) ou fisicamente (fiber/copper)
2. Configure sua rede para anunciar a "Maxihost" como um de seus provedores de internet
3. Decida quando rotear o seu tráfego de entrada através da Maxihost
4. O tráfego de ataque é filtrado para garantir que apenas o tráfego confiável atinja a sua rede



Características Técnicas

- Solução BGP com opção de roteamento estático
- Capacidade de mitigação de 1.44 Tbps
- Conexão via GRE ou camada física
- Redes de centros de mitigação globalmente distribuídas
- Monitoramento e proteção aos ataques das camadas 3 e 4
- Solução assimétrica - via única de ingresso ao tráfego, através da Maxihost

PFN - Modelo OSI

Descrição das camadas OSI: a recomendação X.200 descreve sete camadas, rotuladas de 1 a 7. A camada 1 é a camada mais baixa neste modelo. A PFN protege as camadas 3 e 4: UDP Flood, SYN Flood, DNS Query Flood, ICMP Flood, ACK Flood, TCP Flood e IGMP Flood.

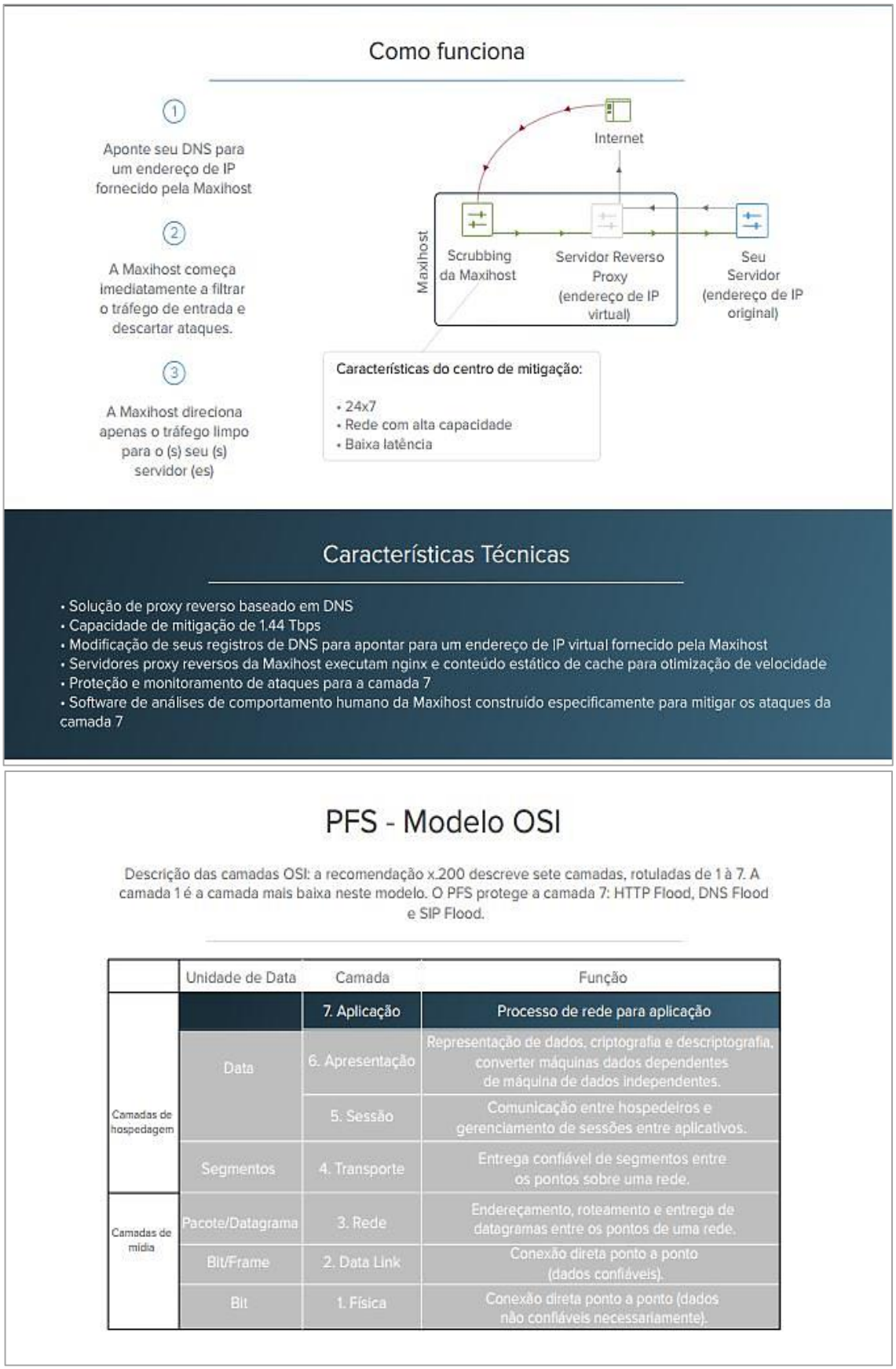
	Unidade de Data	Camada	Função
Camadas de hospedagem	Data	7. Aplicação	Processo de rede para aplicação.
		6. Apresentação	Representação de dados, criptografia e descriptografia, converter máquinas de dados dependentes de máquina de dados independentes.
		5. Sessão	Comunicação entre hospedeiros e gerenciamento de sessões entre aplicativos.
	Segmentos	4. Transporte	Entrega confiável de segmentos entre os pontos de uma rede.
Camadas de mídia	Pacote/Datagrama	3. Rede	Endereçamento, roteamento e entrega de datagramas entre os pontos de uma rede.
	Bit/Frame	2. Data Link	Conexão direta ponto a ponto (dados confiáveis).
	Bit	1. Física	Conexão direta ponto a ponto (dados não confiáveis necessariamente).

Protection for Services
(PFS)

Protege qualquer serviço, o tempo todo. A solução de proteção para redes da Maxihost protege serviços e aplicações de todos os tipos de ataques DDoS. Proteção contra HTTP Flood, DNS Flood, SIP Flood e muitos outros.

Benefícios da PFS

- Mitigação 24x7 com SLA garantido
- Baixa latência - conecte-se ao centro de mitigação mais próximo à você
- Não é necessário nenhum hardware ou software adicional. Utilize apenas sua infraestrutura existente
- Portal de usuário baseado na web - permite o monitoramento em tempo real
- Compatível com os serviços de qualquer lugar do mundo
- Informações sobre ataques disnponíveis em um painel de controle



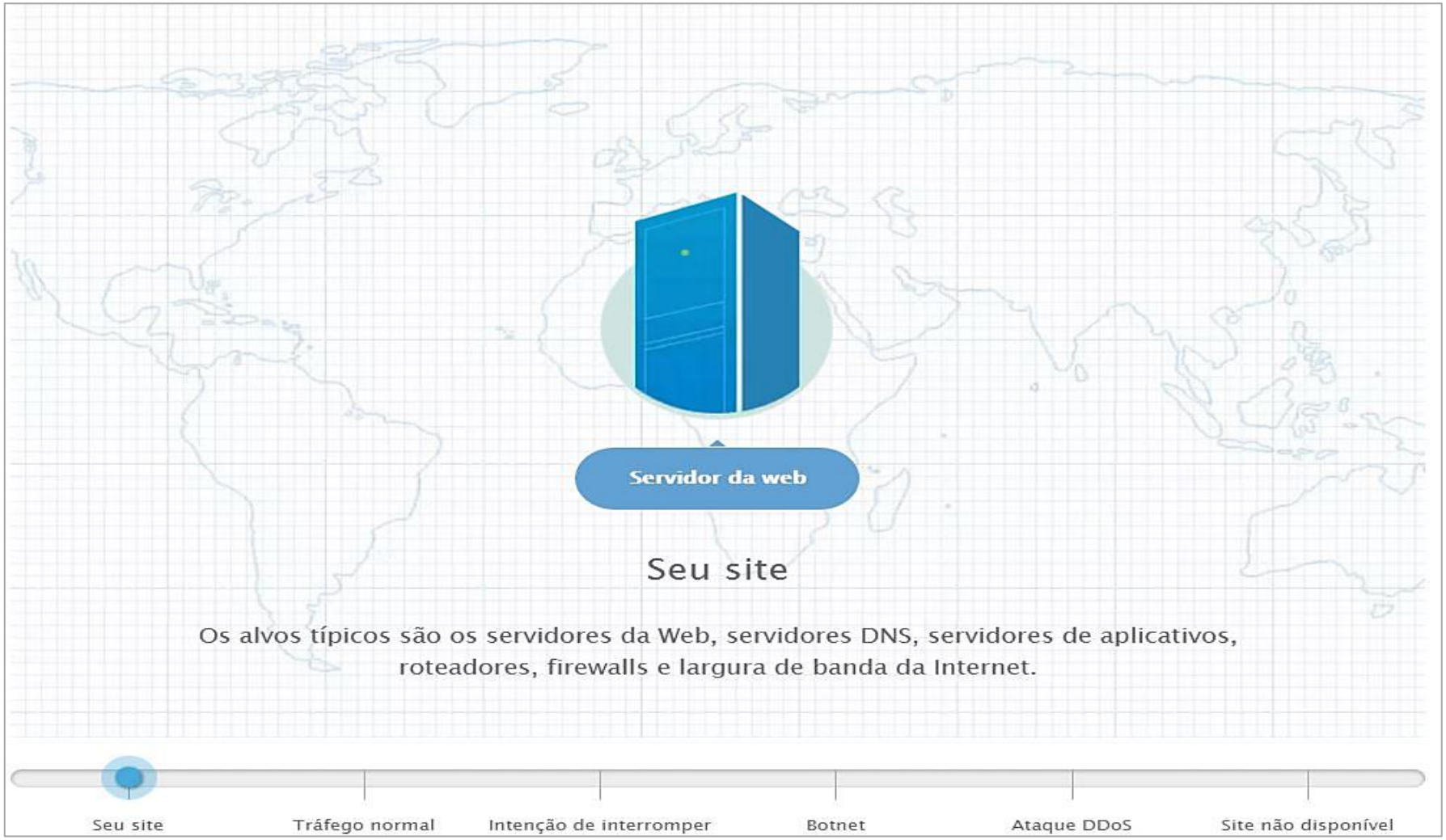
Fonte: *Maxihost* (2016).

ANEXO D - PLANOS E ACORDO *SERVICE LEVEL AGREEMENT* (SLA)

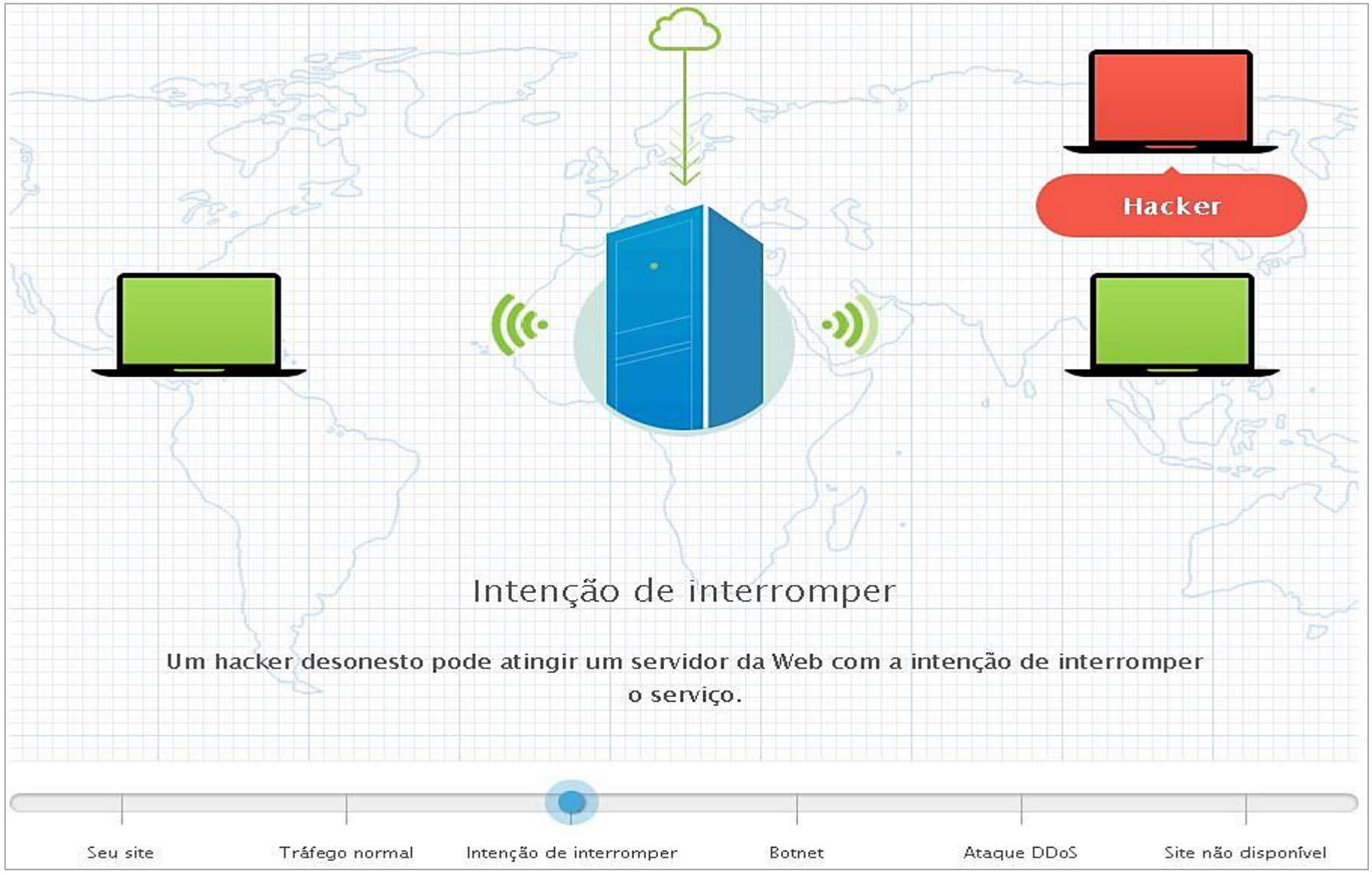
	Anti-DDoS	Anti-DDoS PRO	Anti-DDoS PRO II	Anti-DDoS BGP
Limite de ataque	1G/100K PPS internacional*	20G/200K PPS internacional* +R$100/mês/1 Gigabit/seg	40G/400K PPS internacional* +R$100/mês/1 Gigabit/se	40G/400K PPS internacional* +R$500/mês/5 Gigabit/seg
	100Mbps/10K PPS nacional*	1G/100K PPS nacional* +R$100/mês/100 Mbp	2G/200K PPS nacional* +R$100/mês/100 Mbps	2G/200K PPS nacional* +R$1.000/mês/1 Gigabit/seg
Duração do ataque	Ilimitado	Ilimitado	Ilimitado	Ilimitado
Quantidade de IP	Ilimitado	Ilimitado	Ilimitado	Ilimitado
Tipo do ataque	Todos	Todos	Todos	Todos
Detecção e auto mitigação	Sim	Sim	Sim	Sim
Pontos de mitigação	São Paulo (BR) Los Angeles (EUA) Ashburn (EUA)	São Paulo (BR) Los Angeles (EUA) Ashburn (EUA)	São Paulo (BR) Los Angeles (EUA) Ashburn (EUA)	São Paulo (BR) Los Angeles (EUA) Ashburn (EUA)
Mitigação permanente	Sim	Sim	Sim	Sim
Customização DDoS	Não	Sim	Sim	Sim
Customização Firewall	Não	Sim	Sim	Sim
Mensalidade	R$90	R$490	R$690	Consulte http://maxihost.com.br/contato/

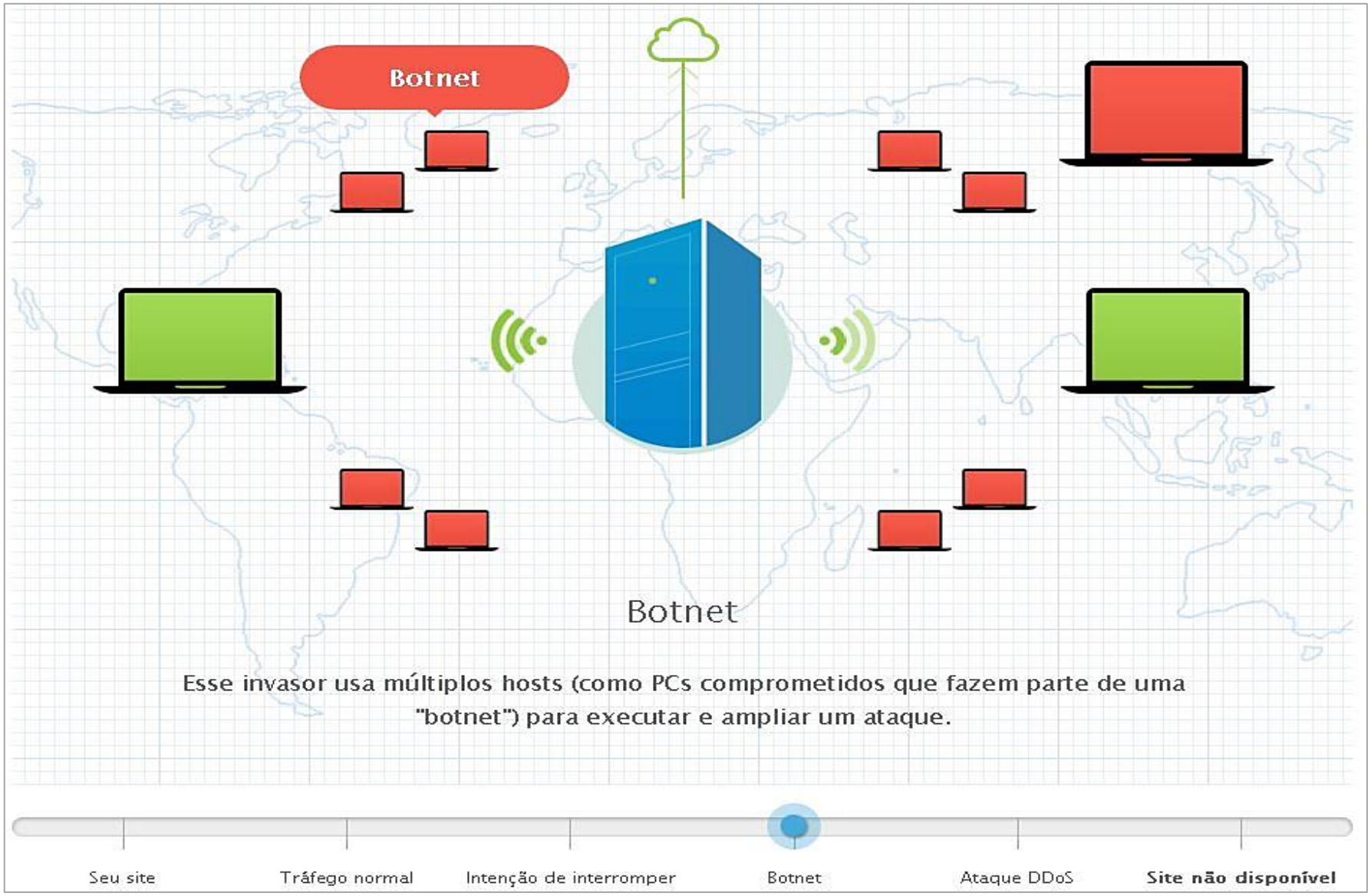
Fonte: Adaptado de *Maxihost* (2016)

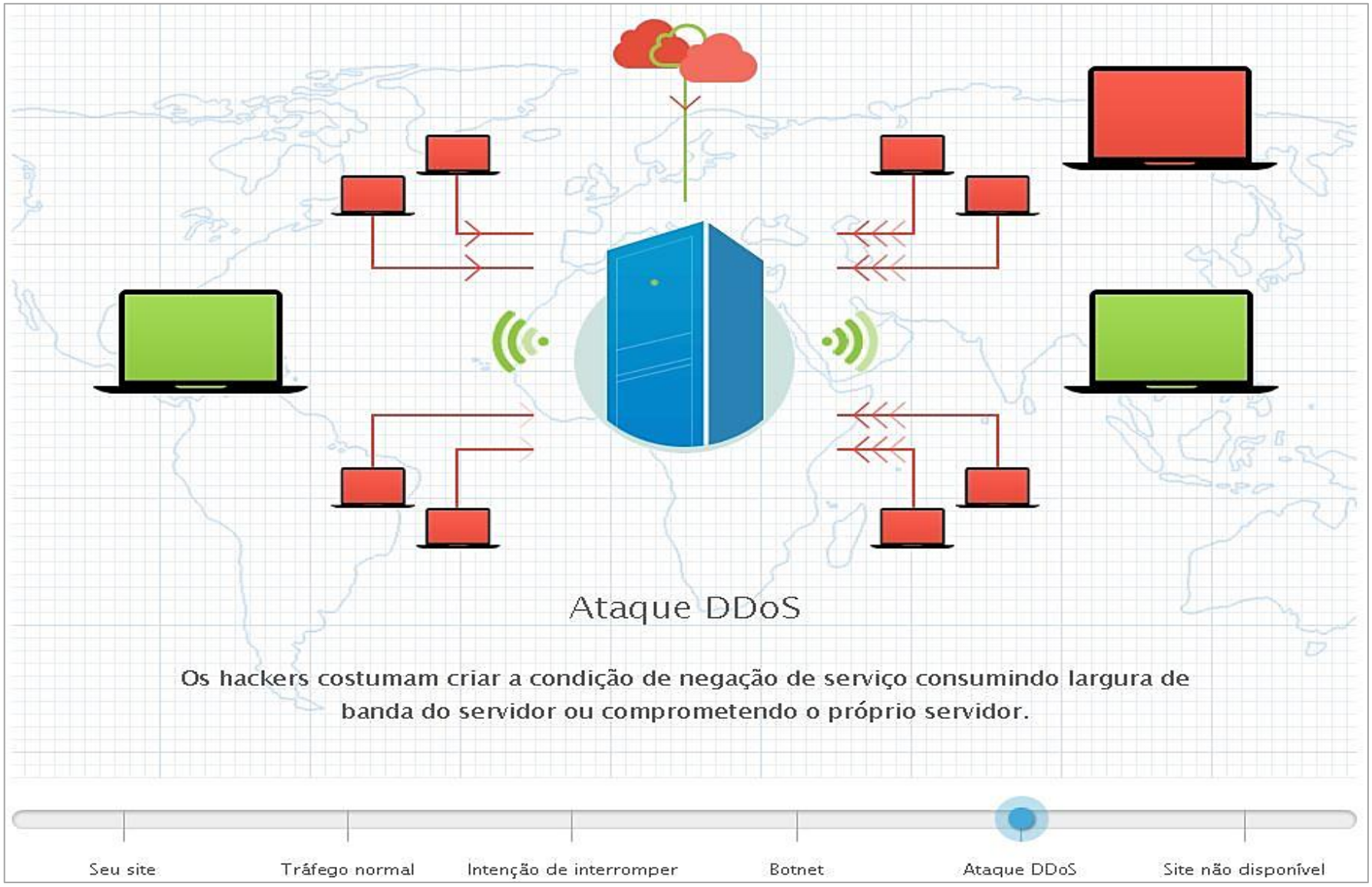
ANEXO E - FUNCIONAMENTO DE UM ATAQUE DISTRIBUÍDO DE NEGAÇÃO DE SERVIÇO

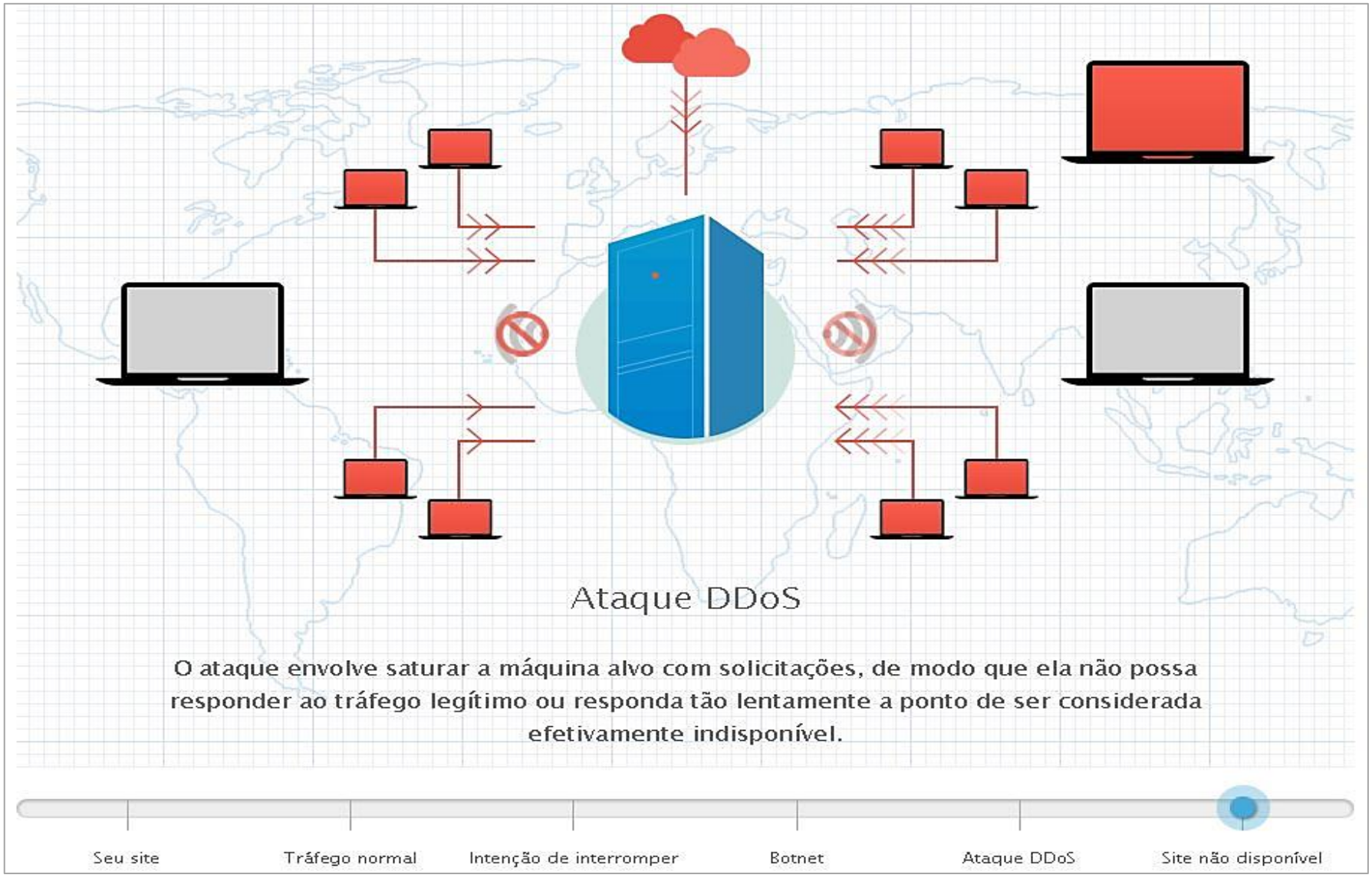



Usuário do site
Usuário do site
Tráfego normal
Os usuários acessam facilmente seus produtos e serviços.
Seu site
Tráfego normal
Intenção de interromper
Botnet
Ataque DDoS
Site não disponível


Hacker
Intenção de interromper
Um hacker desonesto pode atingir um servidor da Web com a intenção de interromper o serviço.
Seu site
Tráfego normal
Intenção de interromper
Botnet
Ataque DDoS
Site não disponível

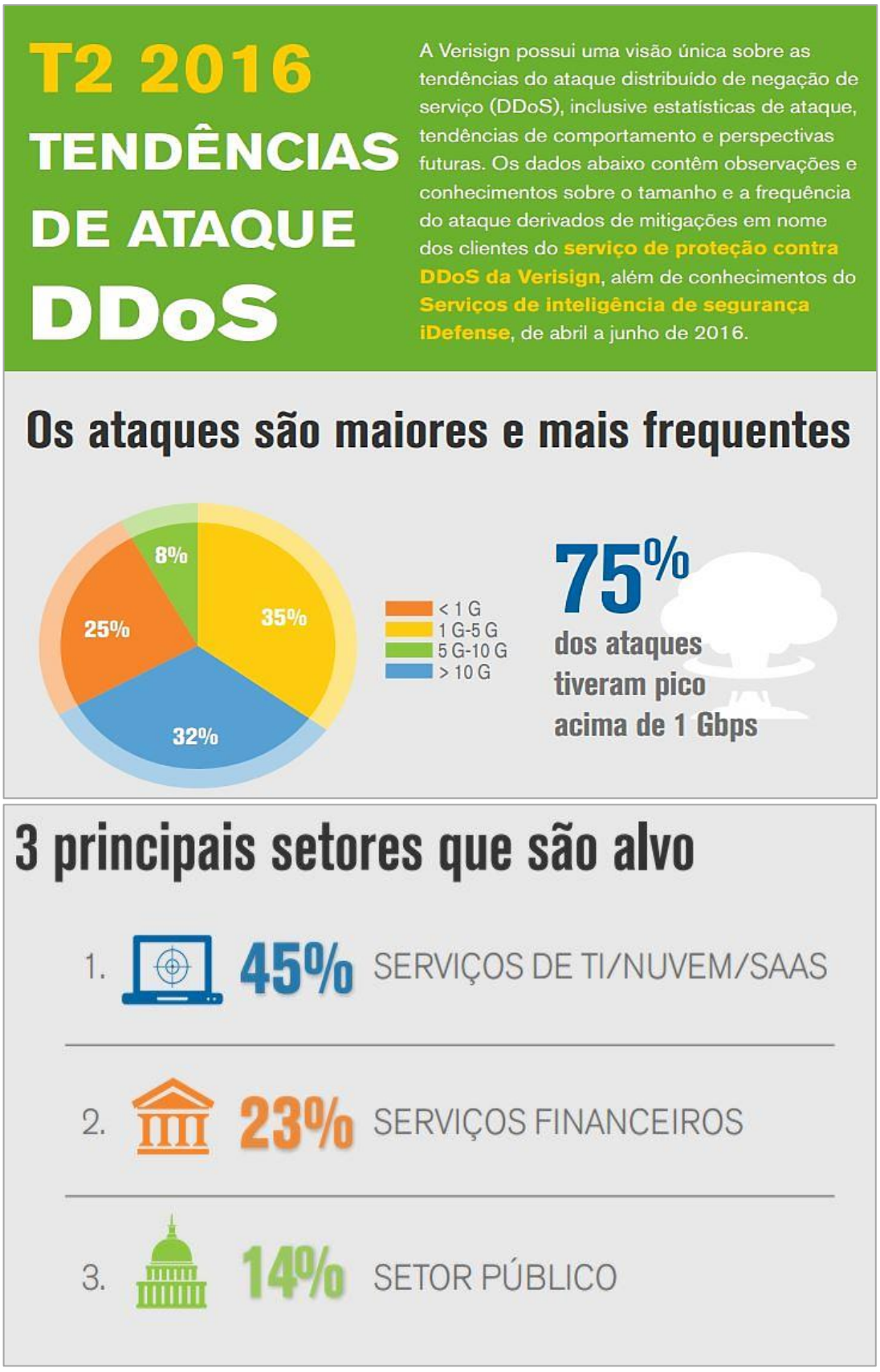

Botnet
Botnet
Esse invasor usa múltiplos hosts (como PCs comprometidos que fazem parte de uma "botnet") para executar e ampliar um ataque.
Seu site
Tráfego normal
Intenção de interromper
Botnet
Ataque DDoS
Site não disponível


Ataque DDoS
Os hackers costumam criar a condição de negação de serviço consumindo largura de banda do servidor ou comprometendo o próprio servidor.
Seu site
Tráfego normal
Intenção de interromper
Botnet
Ataque DDoS
Site não disponível



Fonte: *Verisign* (2016).

ANEXO F – RELATÓRIO SOBRE TENDÊNCIAS DO ATAQUE DDoS



Fonte: *Verisign* (2016).