UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO SUPERIOR DE TECNOLOGIA EM SISTEMAS DE TELECOMUNICAÇÕES

ALEXSANDER WEIGERT
GELASIO ONOFRE DE CASTILHO JUNIOR

UTILIZAÇÃO DE *FIREWALL* EM APLICAÇÃO DE SEGURANÇA E FERRAMENTAS GERENCIAIS

TRABALHO DE CONCLUSÃO DE CURSO

CURITIBA
2017

ALEXSANDER WEIGERT
GELASIO ONOFRE DE CASTILHO JUNIOR

UTILIZAÇÃO DE *FIREWALL* EM APLICAÇÃO DE SEGURANÇA E FERRAMENTAS GERENCIAIS

Trabalho de Conclusão de Curso de Graduação, apresentado ao Curso Superior de Tecnologia em Sistemas de Telecomunicações, do Departamento Acadêmico de Eletrônica, da Universidade Tecnológica Federal do Paraná – UTFPR, como requisito parcial para obtenção do título de Tecnólogo.

Orientador: Prof. Dr. Kleber Kendy Horikawa Nabas

CURITIBA
2017

TERMO DE APROVAÇÃO

ALEXSANDER WEIGERT
GELASIO ONOFRE DE CASTILHO JUNIOR

UTILIZAÇÃO DE *FIREWALL* EM APLICAÇÃO DE SEGURANÇA E FERRAMENTAS GERENCIAIS

Este trabalho de conclusão de curso foi apresentado no dia 08 de junho de 2017, como requisito parcial para obtenção do título de Tecnólogo em Sistemas de Telecomunicações, outorgado pela Universidade Tecnológica Federal do Paraná. Os alunos foram arguidos pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

_____
Prof. Dr. Danillo Leal Belmonte
Coordenador do Curso de
Tecnologia em Sistemas de Telecomunicações

_____
Prof. M.Sc. Sérgio Moribe
Responsável pela Atividade de Trabalho de Conclusão de Curso
Departamento Acadêmico de Eletrônica

BANCA EXAMINADORA

_____
Prof. M.Sc. Omero Francisco Bertol
UTFPR

_____
Prof. Dr. Edenilson José da Silva
UTFPR

_____
Prof. Dr. Kleber Kendy Horikawa Nabas
Orientador – UTFPR

"A Folha de Aprovação assinada encontra-se na Coordenação do Curso"

AGRADECIMENTO

Agradeço em primeiro lugar ao Grande Mestre, Aquele que permite que todas as coisas se concretizem, nosso único e verdadeiro Deus.

Em segundo lugar agradeço a todas as pessoas que diretamente ou indiretamente, contribuíram para a construção dos meus valores: meus Pais, Amigos e em especial uma pessoa que não está entre nós Maria Zoni Weigert, sinto sua falta, aos mestres do passado e todos os que compartilharam um pouco do que sabem comigo.

Não vou deixar de agradecer a compreensão de pessoas especiais, quando minha presença não foi possível e quando minha preocupação e atenção pareciam se voltar exclusivamente para o trabalho, obrigado Dayane, obrigado Mãe e Pai. Ao amigo e orientador Prof. Dr. Kleber Kendy Horikawa Nabas que nos incentivou a continuar com o projeto apesar das dificuldades, o nosso mais sincero agradecimento.

Alexsander Weigert

Agradeço ao Grande Arquiteto, senhor supremo e soberano, que me permitiu chegar até aqui.

Agradeço a todos os professores que tive a oportunidade de conviver durante estes anos de curso.

Agradeço a minha família em especial aos meus pais Gelasio Castilho e Amélia de Castilho, pois através de seus exemplos me tornei quem sou.

Agradeço a minha mulher, Barbara Soeira, por todo seu suporte e compreensão para a concretização desta etapa.

Gelasio Onofre de Castilho Junior

RESUMO

WEIGERT, Alexsander; CASTILHO JUNIOR, Gelasio Onofre de. **Utilização de *firewall* em aplicação de segurança e ferramentas gerenciais**. 2017. 62f. Trabalho de Conclusão de Curso (Curso Superior de Tecnologia em Sistemas de Telecomunicações), Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2017.

A segurança da informação está relacionada com a proteção dos valiosos dados de um indivíduo ou de uma determinada empresa, com a alta demanda na busca por integridade das informações e a confidencialidade de sistemas, como exemplo: transações bancárias, agendamento de uma consulta médica ou um simples acesso a um *site* de busca. As atividades vão convergindo a uma dependência da conectividade, devido a isso, implementação de tecnologias voltadas a área de segurança em telecomunicações estão em constante transformação, esses processos evolucionários têm relevância e importância nos ambientes corporativos. Ter privacidade e segurança nas informações em um ambiente corporativo só é possível com as ferramentas certas, aliadas a uma política de segurança bem elaborada e amplamente divulgada, praticada por cada um dos colaboradores. Com avanço da tecnologia as informações estão cada vez mais acessíveis, o que facilitou o acesso a informações por parte de criminosos que visam roubos de informações confidenciais, desvio eletrônico de recursos e congestionamento de serviços. O objetivo deste trabalho é demonstrar quais ferramentas podem ser utilizadas na área de segurança de redes e os conceitos de um sistema chamado *firewall,* para isso foi utilizado uma aplicação de um sistema de gerenciamento unificado chamado de Check Point, para demonstrar como funciona a detecção e o gerenciamento destes *softwares*, que geralmente operam sob uma arquitetura de segurança unificada, que permite um único agente que pode ser gerenciado a partir de um único console de gerenciamento.

Palavras chave: Gestão de Segurança. Gerenciamento de Redes. Ambiente corporativo. *Firewall*.

ABSTRACT

WEIGERT, Alexsander; CASTILHO JUNIOR, Gelasio Onofre de. **Use of firewall in security application and management tools**. 2017. 62f. Trabalho de Conclusão de Curso (Curso Superior de Tecnologia em Sistemas de Telecomunicações), Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2017.

Information security is related to the protection of valuable data of an individual or a particular company, with the high demand in the search for information integrity and the confidentiality of systems, such as: banking transactions, scheduling a medical consultation or a Simple access to a search engine. The activities are converging to a dependence of connectivity, due to this, implementation of technologies focused on the area of security in telecommunications are in constant transformation, these evolutionary processes have relevance and importance in corporate environments. Having privacy and security in the information in a corporate environment is only possible with the right tools, coupled with a well-developed and well-publicized security policy practiced by each of the employees. With the advancement of technology, information is increasingly accessible, facilitating access to information by criminals seeking theft of confidential information, electronic diversion of resources, and congestion of services. The objective of this work is to demonstrate which tools can be used in the area of network security and the concepts of a system called firewall, for this was used an application of a unified management system called Check Point, to demonstrate how the detection and The management of these softwares, which usually operate under a unified security architecture, which allows a single agent that can be managed from a single management console.

Keywords: Security Management. Network Management. Corporate environment. Firewall.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE GRÁFICOS

LISTA DE ABREVIATURAS, SIGLAS E ACRÔNIMOS

ABNT	Associação Brasileira de Normas Técnica
APIs	*Application Programming Interface*
APTs	*Advanced Persistent Threats*
ARP	*Address Resolution Protocol*
AT&T	*American Telephone and Telegraph*
BOTs	*Software* Malicioso
CID	Confidencialidade, Integridade e Disponibilidade
CLIs	*Command Line Interface*
CRM	*Customer Relationship Management*
DHCP	*Dynamic Host Configuration Protocol*
DLP	*Data Loss Preventio*
DMZ	*Demilitarized Zone*
DNS	*Domain Name System*
EBCDIC	*Extended Binary Coded Decimal Interchange Code*
FDDI	*Fiber Distributed Data Interface*
FTP	*File Transfer Protocol*
GB	*Gigabytes*
HTTP	*Hypertext Transfer Protocol*
ICMP	*Internet Control Message Protocol*
ICS	*Industrial Control System*
IEC	*International Electrotechnical Commission*
IEEE	*Institution of Electrical and Electronics Engineers*
IP	*Internet Protocol*
IPS	*Internet Protocol Secure*
ISO	*International Organization for Standardization*
ITU	*International Telecommunication Union*
LAN	*Local Area Network*
MAN	*Metropolitan Area Network*
MP’s	Módulos Processadores
NBR	Norma Brasileira Regulamentadora
NDR	*Network Data Representation*
OSI	*International Organization for Standardization*
RARP	*Reverse Address Resolution Protocol*
RCP	*Remote Call Procedure*
SCADA	*Supervisory Control and Data Acquisition*
SCP	*Session Control Protocol*
SDP	*Sockets Direct Protocol*
SMLI	*Stateful Multi-Layer Inspection*
SSH	*Secure Shell*
TCP	*Transmission Control Protocol*
TI	Tecnologia da Informação
UDP	*User Datagram Protocol*
URL	*Uniform Resource Locator*
WAN	*Wide Area Network*

SUMÁRIO

1 INTRODUÇÃO

A área de Sistema de Telecomunicações vem desempenhando um papel muito importante, como: melhorar desempenho das redes; criando aplicações de serviços que facilitam a vida dos usuários; convergência de telefonia, imagem e dados, em uma única matriz de transferência de dados. Há uma crescente dependência em obter-se e divulgar informação de maneira instantânea, a velocidade e as aplicações para o uso da Internet, tem gerado uma carência em velocidade e banda.

Com base nessas necessidades, diversos conceitos de telecomunicações vêm sendo desenvolvidas para responder essa pergunta, “Como garantir a segurança e a integridade das minhas informações? ”

A implementação de tecnologias voltada à área de telecomunicações, estão em constante transformação e tem relevante importância nos ambientes corporativos, para cada aplicação, seja para uso doméstico ou empresarial, hoje existem ferramentas para proteger e garantir a integridade das informações, para muitos o maior patrimônio é a informação armazenada em um computador.

1.1 TEMA

Em redes corporativas, é possível evitar que os usuários acessem serviços ou sistemas indevidos, além de ter o controle sobre as ações realizadas na rede, sendo possível até mesmo descobrir quais usuários as efetuaram. Visando promover a integração desta tecnologia com os conhecimentos obtidos durante os estudos acadêmicos na área de redes, esse projeto proporcionará a capacitação dos membros para uso de novas habilidades que envolvem os sistemas de telecomunicações, foco de estudo dos membros integrantes da equipe de desenvolvimento, que com essa vivência poderão ampliar seu campo de atuação.

1.2 DELIMITAÇÃO DO ESTUDO

A análise demonstrada neste trabalho de concussão de curso, foi realizada em uma empresa do ramo alimentício, que a trinta e cinco anos está no mercado, foram realizados no ano de 2016, como proposta para demonstração do sistema de gerenciamento de segurança de redes *Chek Point.* Por se tratar de informações específicas e vincular os resultados obtidos a informações estratégicas desta empresa, optou-se em não divulgar nome ou ramo de atuação.

1.3 PROBLEMAS

Invasões nos sistemas internos das empresas têm preocupado os profissionais da área de segurança de redes. Ataques que antes visavam apenas reafirmar a ousadia dos *hackers*[1], hoje se mostram com objetivos mais claros, como roubos de informações confidenciais, desvio eletrônico de recursos e congestionamento de serviços.

Observa-se que a demanda por controle e segurança de rede tem aumentado e com isso surgem alguns questionamentos: Qual o melhor sistema de segurança a ser implantado? Onde, dentro da LAN[2], esse sistema deveria ser implantado? Depois de implantado quais serão os benefícios desse sistema?

Perante o exposto, será apresentado um estudo sobre o *firewall,* assim como a importância de implementar esse sistema no âmbito corporativo. Porém é importante salientar que não é o único dispositivo de segurança de rede, contudo um dos mais importantes.

Através do estudo do funcionamento do *firewall,* suas configurações e formas de implementação, será apresentado como uma opção para a resposta das perguntas acima e demonstrar a importância da implantação desse sistema.

---

[1]hacker - Segundo tradução do dicionário (MICHAELIS, 2017) “Uma pessoa que usa seu conhecimento técnico para acesso a sistemas privados”.

[2]LAN (Local Area Network)- Rede local definida como abrangência física de até poucos quilômetros com alta taxa de transferência de dados(SOARES, et al., 1995)

1.4 OBJETIVOS

Para que os sistemas de segurança sejam estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessários, é preciso destacar os seguintes objetivos.

1.4.1 **Objetivo Geral**

Apresentar o conceito de *firewall* e suas aplicações em redes de computadores, explanando as principais ferramentas de segurança que hoje podem auxiliar na segurança das informações e demonstrar a importância da implantação do *firewall* nas redes corporativas, através do estudo das características e dos aspectos técnicos desse sistema, assim como apresentar uma possível solução de *firewall* que de a segurança e o gerenciamento da rede.

1.4.2 **Objetivos Específicos**

Os objetivos específicos têm os seguintes pontos:

1. Apresentar os fatos históricos que intensificaram os esforços na área de segurança da informação, tornando uma das prioridades nas empresas;
2. Expor como as novas tecnologias trazem consigo novas vulnerabilidades:
3. Descrever os conceitos, características e a importância do *firewall* em ambientes corporativos;
4. Expor os principais riscos à segurança dos dados.

1.5 JUSTIFICATIVA

A implementação de equipamentos na rede com o objetivo de promover e garantir a segurança de dados tem sido utilizada cada vez mais pelas empresas e o *firewall* é uma das alternativas para isso, equipamento que agregam recursos como solução viável, a utilização deste equipamento como solução se explica pelas diversas vantagens oferecidas, tais como:

- Serviços de auditoria simultânea capaz de fornecer às empresas o controle sobre o que os usuários podem executar;
- Suporta comando HTTP de filtragem para um controle eficiente sobre como *Web* servidores são acessados, proporcionando uma forte barreira a conteúdos impróprios;
- Capacidades de validação de conteúdo;
- Serviços de inspeção no HTTP que ajudam a proteger contra-ataques baseados na *Web* e outros tipos de "mau uso da porta 80";
- Inclui políticas de bloquear acessos personalizáveis;
- Interface amigável para gerenciamento;
- O *firewall* pode ser usado para ajudar a impedir que sua rede ou seu computador seja acessado sem autorização.

1.6 PROCEDIMENTOS METODOLÓGICOS

A implementação deste projeto será orientada pelos manuais, normas, tutoriais e bibliografias de referência que tratam do escopo do projeto, incluindo o compartilhamento de informações com especialistas da área.

A primeira etapa do trabalho será baseada na contextualização do tema, invasões recentes e motivações que levaram ao desenvolvimento do *firewall,* através de *Sites* da Internet e livros técnicos. Seguido dessa pesquisa, será apresentado o conceito de *firewall,* sua importância, as divisões existentes e os principais *firewall* utilizados nos ambientes corporativos.

Posteriormente, será realizada um estudo para implantação em uma empresa, simulando os impactos e o funcionamento de uma rede com um *firewall,* verificando principalmente os parâmetros que devem ser atribuídos à rede para operação compatível com esta tecnologia.

A última etapa do trabalho será vincular os conhecimentos técnicos adquiridos com as simulações realizadas para que se possa demonstrar os benefícios da implantação de um *firewall* a redes corporativas.

1.7 ESTRUTURA DO TRABALHO

O trabalho terá a estrutura a seguir:

Capítulo 1 - Introdução: Serão apresentados o tema, as delimitações da pesquisa, o problema e a premissa, os objetivos da pesquisa, a justificativa, os procedimentos metodológicos e a estrutura geral do trabalho.

Capítulo 2 – Fundamentação Teórica: Será abordado o conceito de segurança e gerenciamento de acesso, conceito de rede de computadores o conceito de *firewall* e suas variações.

Capítulo 3 – Apresentação e Análise dos Resultados: Tendo como base os procedimentos metodológicos, neste capítulo serão descritos as ferramentas e os resultados que cada módulo pode oferecer, juntamente com um exemplo prático da aplicação dos módulos resultados obtidos e feitas as devidas análises relacionados ao território turístico de Curitiba.

Capítulo 4 – Conclusão: Serão respondidas as perguntas que foram feitas no capítulo 1, evidenciando os resultados obtidos, por meio do trabalho realizado. Além disto, serão sugeridos trabalhos futuros que poderiam ser realizados a partir do estudo realizado.

2 FUNDAMENTAÇÃO TEÓRICA

Toda corporação está vulnerável a ataques provenientes desta conectividade moderna. Os ataques aos sistemas apresentam objetivos diferentes e o seu sucesso depende do grau de segurança dos alvos e da consequente capacidade do hacker em atacá-los. Conforme (ABNT, 17799:2005), o comércio eletrônico é vulnerável a várias ameaças pela rede que podem derivar em atividades fraudulentas, disputas contratuais e divulgação ou modificação de informação.

Com o crescimento da internet e facilidade em se obter informações e ferramentas para ataques, qualquer incidente de segurança atualmente é atribuído a *hackers*, mas não são apenas eles que causam problemas de segurança nos sistemas, os próprios usuários, mesmo sem más intenções, também podem causar danos, por meio de seus erros e/ou ignorância. Segundo (ABNT, 17799:2005), hacker é uma pessoa que tenta acessar sistemas sem autorização, usando técnicas próprias ou não, para que tenha acesso a determinado ambiente para proveito próprio ou de terceiros.

2.1 SEGURANÇA DA INFORMAÇÃO

De acordo com dicionário HOUAISS (2001, p. 2536), segurança é o estado, qualidade ou condição de uma pessoa ou coisa que está livre de perigos, de incertezas, assegurada de danos e riscos eventuais, afastada de todo mal.

Segundo COMER (2001), uma política racional exige que a organização faça uma avaliação sobre o valor das suas informações, sendo muito complexo o desenvolvimento da segurança de rede; e essas informações são diferentes de uma empresa para outra. A respeito disto (ABNT, 17799:2005) afirma que:

> “A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de *software* e *hardware*.”

A norma ABNT NBR ISO/IEC 27002 define segurança da informação como a proteção da informação contra os diferentes tipos de ameaças a fim de minimizar o

risco ao negócio. Existem três aspectos chave da segurança da informação que são sempre lembrados como CID (Confidencialidade, Integridade e Disponibilidade), conforme mostrado na Figura 1.

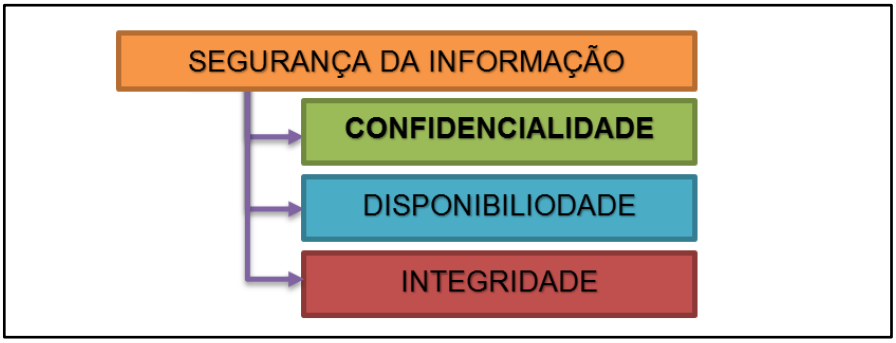


Figura 1 - Segurança da Informação
Fonte: Adaptado de Normas para ABNT NBR ISO/IEC 27002.

Segundo NAKAMURA E GEUS (2007) a integridade, disponibilidade, confidencialidade e sigilo formam as propriedades mais importantes para segurança. “Toda a informação deve chegar aos usuários de forma integra e confiável. Para que isso aconteça, todos os elementos da rede por onde a informação flui até chegar ao seu destino devem estar disponíveis, e devem também preservar integridade das informações" (Nakamura e Geus, 2007, p. 43).

O acesso a rede de computadores, está cada vez mais difundido, e a internet tornou-se o principal e mais rápido meio de iteração mundial. Com a possibilidade de qualquer pessoa ter acesso à Internet, prover a segurança da informação tornou-se essencial, e por consequência o mercado tem visado cada vez mais o desenvolvimento de equipamentos que tenham por objetivo regulamentar o tráfego de dados, assim como realizar um controle das trocas de informações, evitando dessa forma acessos nocivos ou não autorizados de uma rede para outra.

De acordo com CHIAVENATO (2000) apud RIBEIRO, a cultura organizacional conglomera aspectos formais, facilmente perceptíveis, relacionados com as políticas, diretrizes, procedimentos, objetivos, estruturas e tecnologias existentes, e aspectos informais, relacionados com as percepções, sentimentos, atitudes, valores, interações informais e normas grupais, Segundo os conceitos apresentados sobre cultura organizacional, pode-se entender que a cultura da organização é um dos principais ativos de qualquer organização, pois compreende o conjunto de concepções, valores, normas ou premissas da organização.

De acordo com a Norma ABNT NBR ISO/IEC 27002 no item 01. Introdução, apresenta a seguinte definição para o assunto:

> “A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida. Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectado. Como um resultado deste incrível aumento da interconectividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades

O Decreto 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal no seu artigo 2º faz a seguinte conceituação no item II:

> “II - Segurança da Informação: proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaça a seu desenvolvimento. (BRASIL, O Decreto 3.505, de 13 de junho de 2000)”

Segurança na computação é um tema sempre muito discutido, muito porque este está sempre mudando, pois novas ameaças surgem o tempo todo. Segundo NAKAMURA E GEUS (2007) o mundo da segurança é formado por um ciclo, pois novos ataques têm como resposta novas formas de proteção, levando ao desenvolvimento de novas técnicas de ataque e assim sucessivamente.

Para demonstrar como é importante a questão de segurança em redes de computadores, pode-se observar no gráfico 1, o qual traz informações de incidentes reportados ao CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil).

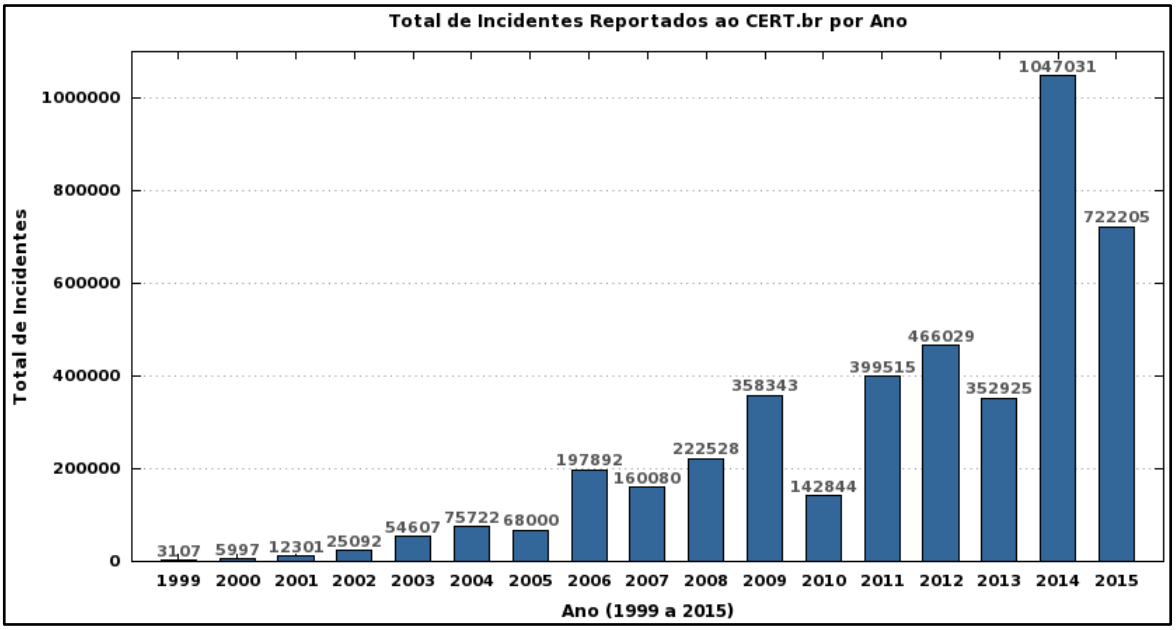


Gráfico 1 - Crescimento dos Incidentes Reportados ao CERT.br
Fonte: CERT.br

O gráfico 1 traz a quantidade de incidentes reportados no período de 1990 até Março de 2015, demonstra que a partir de 2006 os incidentes relatados aumentaram consideravelmente em relação aos anos anteriores, somando os incidentes reportados de 1999 a 2005, tem-se um total de 244.826 incidentes reportados, ou seja, em 2 anos o número de incidentes superou em mais de 30% (31,61%) o número de incidentes nos 7 anos anteriores. Porém como pode ser observado em 2010 o número de incidentes reportados é bem inferior em relação aos anos adjacentes, isto não significa necessariamente que o número de incidentes neste ano foi inferior à média dos anos subsequentes, pois o gráfico só traz os incidentes reportados ao CERT.br. Pode-se estimar que, permanecendo os mesmos perfis de comportamento, em 2014 os números de incidentes ultrapassam a marca de um milhão, demonstrando uma tendência exponencial de crescimento.

Com esse novo ambiente em desenvolvimento, um novo campo de estudos tem estado em evidência, à segurança de redes. Essa área é marcada pela evolução contínua e evolutiva, ou seja, conforme novos ataques surgem novas formas de defesas passam a existir. Sendo assim, pode ser considerado alguns pontos, para que a segurança contínua seja justificada:

- Compreender que as maiorias das invasões são resultado da exploração de vulnerabilidades, ou seja, eles podem ocorrer nas

falhas de implementação do sistema de segurança, inclusão de novas tecnologias e novos sistemas de conectividade;

- As diferentes formas e a facilidade de acesso à Internet, possibilitam novos ataques e por consequência devem ser desenvolvidas novas formas de defesa, o que torna a defesa mais complexa que o ataque. Enquanto em um ataque o criminoso deverá identificar apenas um ponto de falha para prover a invasão no sistema, a defesa deve se preocupar com todos os possíveis pontos de invasão para mitigar os riscos;
- Entender os motivos dos ataques facilita no desenvolvimento de sistemas de segurança. Os ataques podem ter diferentes propósitos, por exemplo, interromper serviços específicos, comprometendo dados ou *software*s, desestabilizar uma rede com o objetivo de coletar informações que serão utilizadas posteriormente em uma nova invasão e o ataque com a finalidade do roubo de dados.

Neste contexto surge o *firewall* como um mecanismo de defesa, controlando e assegurando, a sua maneira e com as suas limitações, os acessos a uma rede.

2.2 CONCEITO DE REDE DE COMPUTADORES

Segundo DANTAS (2002), pode-se considerar redes de comunicação como sendo um ambiente onde um conjunto de dispositivos, enlaces de comunicação e pacotes de *software* permitem que as pessoas e equipamentos possam trocar informações. (SOARES, et al., 1995) classifica “que uma rede de computador é formada por conjunto de módulos processadores MP’s é capaz de trocar informações e compartilhar recursos, interligados por um sistema de comunicação”. Há diferentes conceitos de rede de computadores (LAN, MAN ou WAN).

Mas de acordo com DANTAS (2002) as referências mais comuns são elas: LAN (*Local Area Network*) Rede local definida como abrangência física de até poucos quilômetros com alta taxa de transferência de dados; MAN (*Metropolitan Area Network*)- são redes com características metropolitanas de cobertura geralmente de cidades; WAN (*Wide Area Network*) uma região geograficamente distribuída engloba vasta região como estado, país e continente, possui elevada taxa de erros comparada as LAN’s, devido sua dimensão, chamada popularmente de

internet ou rede mundial de computadores, por sua vez, estas interfaces geram o desenho da tipologia de rede, conforme detalhamento na figura figura 2.

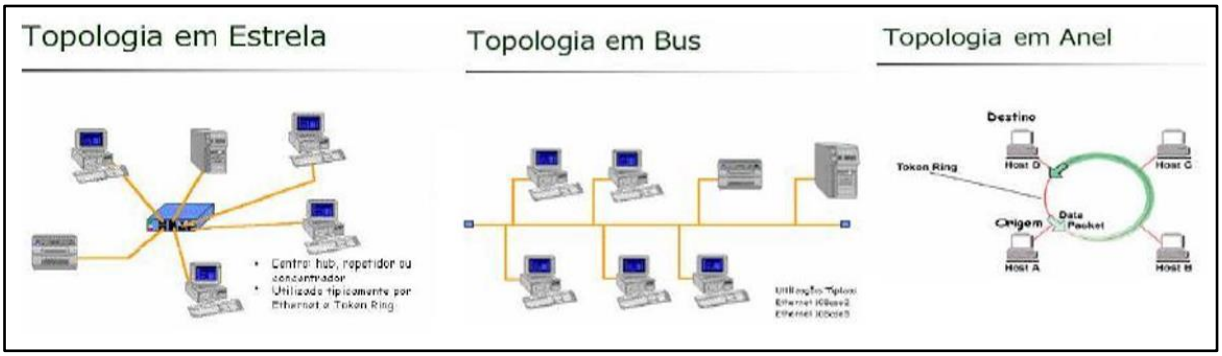


Figura 2 - Tipologias de Redes
Fonte: Redes de computadores. <http://sweet.ua.pt.com.br> Acesso em 25/05/2017.

Hoje temos um conceito novo, que mostra de forma a-espacial que é comumente chamado de nuvem, tem sido utilizado historicamente como uma metáfora da Internet. Este uso foi originalmente derivado de sua representação em diagramas de rede, com um esboço de uma nuvem, usado para representar o transporte de dados através de *backbones*, pertencentes à nuvem (RITTINGHOUSE e RANSOME, 2009).

2.2.1 **O Modelo de Referência OSI**

O modelo OSI, ou interconexão de sistemas abertos (*Open System Interconnection*) foi a mola propulsora para o desenvolvimento das redes de computadores. A primeira rede de computadores denominada ARPAnet em 1960 se comunicava em 16 sistemas fechados injetados pelos seus próprios Processadores de Interface de Mensagem (*interface message processors*) – IMPs. Por isso, tanto a rede quanto a informática eram restritas a áreas militares e centros universitários de pesquisas. Com intuito de expandir a rede, foi projetado e desenvolvido o modelo de referencia (OSI) utilizado até hoje que carregou e impulsionou toda a revolução digital que estamos vivendo.

Segundo Tanenbaum (2011, p.45), o “OSI” é um Modelo de Referência composto por sete camadas, sendo, convencionalmente, iniciada pela 7ª - Camada de Aplicação; 6ª – Apresentação; 5ª – Sessão; 4ª –Transporte; 3ª – *Network* ou Rede; 2ª – *Data Link* ou Enlace de Dados e; 1ª – Física. Na figura 3 esta

representado os ver os sete níveis da divisão OSI e os tipos de protocolos envolvidos em cada camada.

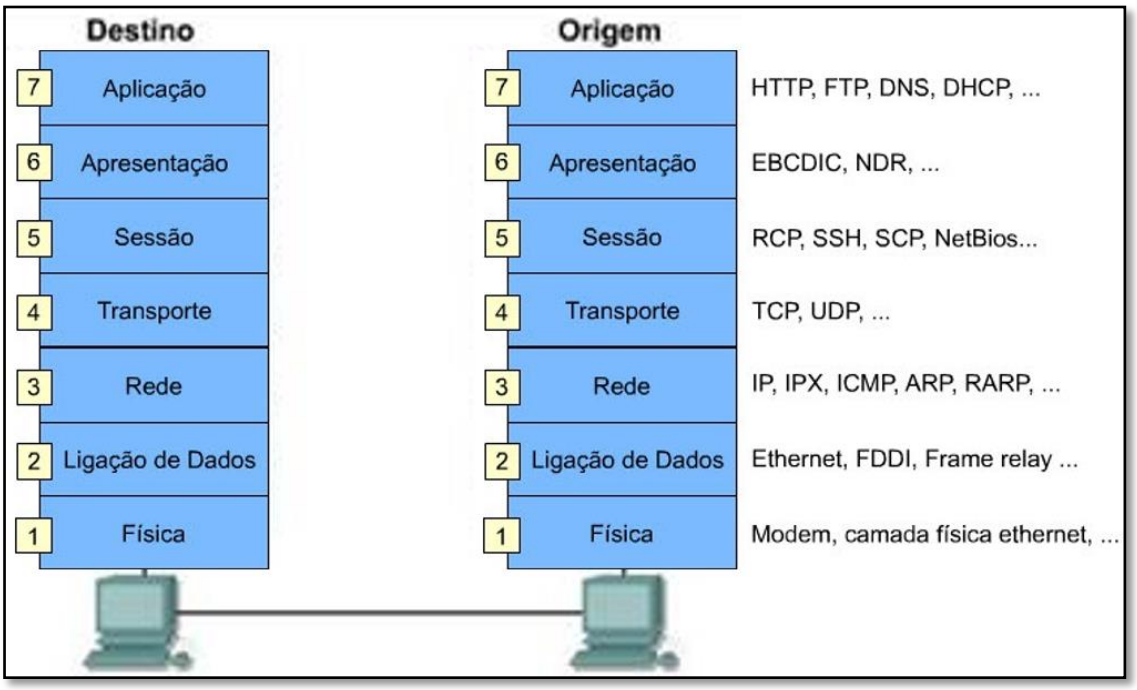


Figura 3 - Modelo de Referência OSI
Fonte: Raul Salustiano. <http://raulsuport.blogspot.com.br> Acesso em 22 maio.2017.

2.3 CONCEITO DE *FIREWALL*

Um *firewall* pode auxiliar e impedir que *hackers* ou *software*s mal-intencionados (*worms*) consigam acesso a um computador por meio de uma rede ou da Internet. Um *firewall* também pode ajudar a impedir o computador de enviar *software* mal-intencionado para outros computadores.

Desenvolvido pela Bell Labs em meados de 1980, a pedido de uma das maiores empresas de telecomunicações do mundo a AT&T, o primeiro *firewall* do mundo foi desenvolvido com o objetivo de “filtrar” informações que entravam e saiam da sua rede empresarial, de forma que fossem flexíveis para a manipulação seguindo especificações presentes as regras definidas pelos cientistas e desenvolvedores da Bell Labs (NETO, 2004, p. 10).

Desde então, mesmo os meios tecnológicos estarem em crescente desenvolvimento, um *firewall* continua obtendo os mesmos conceitos, mas contendo alguns aprimoramentos. Existem basicamente três classes de *firewall* que são filtro de Pacotes, NAT e o Híbrido.

2.3.1 *Firewall* Filtro de Pacotes

É o tipo de *firewall* que filtra todo o tráfego direcionado a ele mesmo ou a rede local a qual ele isola, da mesma forma, é responsável por filtrar os pacotes que ele, ou a rede, emitem.

- *INPUT*: Pacotes que chegam ao *host*;
- *OUTPUT*: Pacotes que saem do *host*;
- *FORWARD*: O que chega a um host e precisa ser redirecionado a um outro host ou outra interface de rede (NETO, 2004).

2.3.2 *Firewall* NAT

Tem a finalidade de manipular a rota do tráfego, aplicando a tradução de endereçamento sobre os pacotes. Isso possibilita a manipulação dos endereços de origem e destino entre outras coisas.

- *PREROUTING*: Quando há necessidade de realizar alterações em pacotes antes serem roteados ao seu destino;
- *POSTROUTING*: Quando há necessidade de realizar alterações depois que os pacotes forem roteados ao seu destino;
- *OUTPUT*: Realiza a verificação em pacotes emitidos pelo host *Firewall* (NETO, 2004).

2.3.3 *Firewall* Híbrido

É a opção de *Firewall* que seria uma união entre as outras duas classes citadas anteriormente, ou seja, “agrega a si tanto funções de filtragem de pacotes quanto de NAT.” (NETO, 2004, p. 13).

- *PREROUTING*: Modifica os pacotes antes deles serem roteados;
- *OUTPUT*: Modifica pacotes gerados localmente antes de serem roteados

Um *firewall* é uma combinação de *hardware* e *software* que isola uma rede interna de outra rede “externa”, a internet em geral, selecionando alguns pacotes -

permitindo alguns e bloqueando outros. Apesar desse tipo de dispositivo ser mais usado em ambiente empresarial, sua utilização está tomando uma nova tendência diante do crescimento dos crimes virtuais.

Figura 4 - Ilustração de uma Rede com *Firewall* Impremetado
Fonte:<http://www.databranch.com/managed-services/managed-*Firewall*olean> Acesso em 22 de maio.de 2016.

Firewall pode ser definido, de acordo com NAKAMURA e GEUS (2007), como “componente ou conjunto de componentes que restringe o acesso entre uma rede protegida e a *Internet*, ou entre outros conjuntos de redes”, como observado na figura 4.

Segundo FREIRE (2004), uma política de segurança adequada é fundamental para a configuração de um firewall. “A política necessita definir quais ações de proteção e procedimentos de gerência de riscos necessitam ser tomadas para proteção do patrimônio da corporação” (FREIRE, 2004).

> “Assim como o guardião, um firewall bem implementado é aquele que, através de um controle baseado em filtros de tráfego, permitirá acesso restrito a determinadas portas e executará o bloqueio de todos os demais serviços a fim de evitar acesso não autorizado de visitantes indesejáveis. Para executar tal tarefa, o firewall necessita funcionar como um ponto único de entrada.” (FREIRE, 2004).

Freire (2004) refere-se um ponto único de entrada ao pensamento de um ambiente conectado à Internet.

Com base na definição de NAKAMURA e GEUS (2007), é possível compreender que *firewall* vai além de uma simples barreira de proteção contra-ataques externos. O *firewall* pode ser utilizado como uma proteção dentro da rede, controlando de tráfegos a servidores específicos, como demostrado na figura 5.

Existem três tipos principais de *firewall*:

a) Firewall em nível de pacote: analisa as informações contidas no cabeçalho dos pacotes e de acordo com as regras especificadas pelo administrador, determinam se o pacote será aceito ou descartado. Esse *firewall* funciona nas camadas de rede e de transporte;

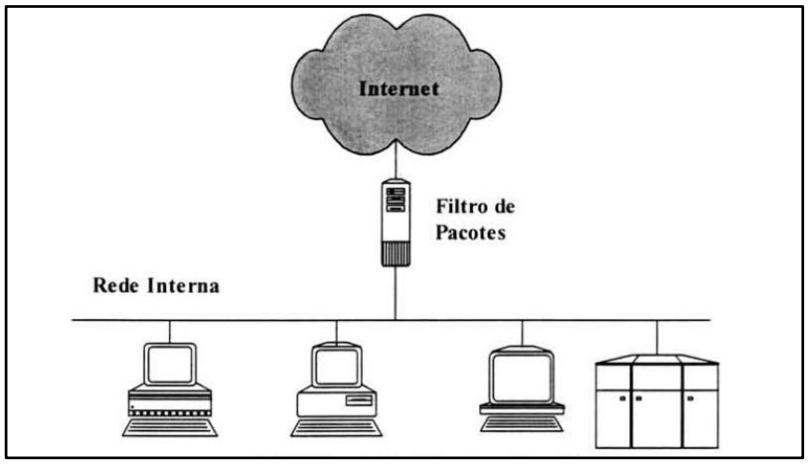


Figura 5 - Exemplo de um *Layout* de Rede com Filtro de Pacotes
Fonte: SPONH, 1997.

b) Firewall em nível de pacotes baseado em estados: também chamado de *stateful packet filter*. O que difere esse sistema do primeiro é a tomada da decisão se o pacote será aceito ou não, a qual é realizada baseada em dois pontos: nas informações do cabeçalho do pacote (assim como o *firewall* a nível de pacotes) e uma tabela de status que guarda o estado das conexões.

c) O *firewall* atuando como filtro de pacotes, como ilustrado na figura 5, ele é instalados em um nível de aplicação, que funciona nas camadas de aplicação, sessão e transporte. Também conhecido como servidor *proxy*, proporciona tomada de decisões baseados nos dados da aplicação, além da análise de cabeçalhos TCP, UDP e IP.

2.4 ARQUITETURA

O principal objetivo de um *firewall* é garantir que todos os dados que trafeguem de uma rede para outra passem obrigatoriamente por ele. Para isso é aconselhável realizar uma avaliação da arquitetura no qual o sistema será implantado, assim como o grau de segurança exigido, podendo ser utilizado quantos níveis de acesso forem necessários para adequar esse sistema.

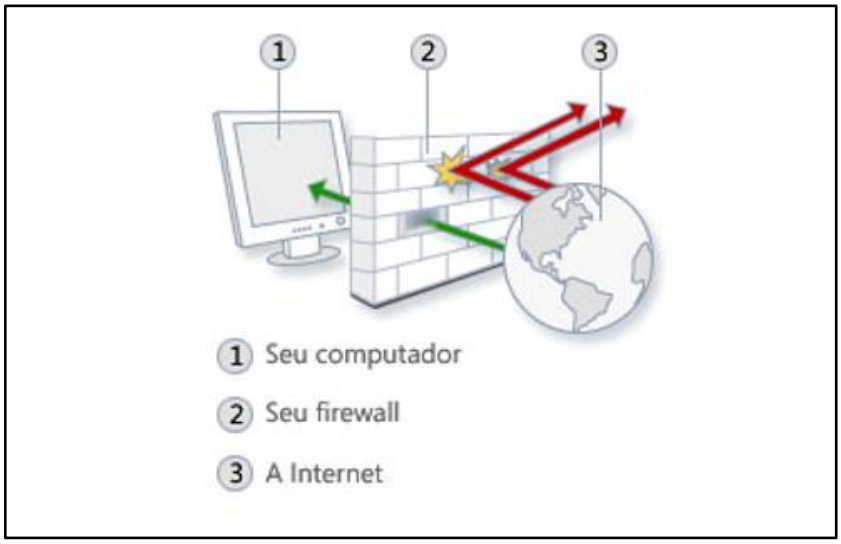


Figura 6 - Ilustração de um *Firewall* na Rede
Fonte: <http://www.ccompany.com.br/firewall.htm> Acesso em 22 de maio de 2017.

Existem algumas arquiteturas que servem como base para a implantação de um *firewall* , tais como: *Dual-homed Host, Screened Host e Screened Subnet*.

A arquitetura *dual-homed* host pode ser implementada por um *host* que apresenta duas interfaces de rede, uma para LAN e outra para a rede externa, se tornando a única porta de entrada. Nessa arquitetura o roteamento é desabilitado, fazendo com que os pacotes não possam ser roteados entre as redes, garantindo o isolamento do tráfego. De acordo com Zwicky, Cooper e Chapman (2000), a arquitetura dual-homed host é indicada para: uma rede que possua um tráfego pequeno para Internet, o tráfego para a Internet não seja vital para o negócio da empresa e que a mesma não provenha nenhum serviço para a Internet.

A arquitetura *screened* host é formada por um filtro de pacotes que atua em um primeiro nível de defesa e é responsável por restringir conexões externas que não sejam direcionadas a um host especifico, chamado *bastion host* (o único host da rede interna acessível por hosts externos), ou seja, os usuários externos que

quiserem acessar os sistemas internos deverão se conectar primeiramente com o *bastion host*. De acordo com NAKAMURA e GEUS (2007) um problema dessa arquitetura é que, se o *bastion host* for comprometido o invasor terá acesso total à rede interna da organização.

A arquitetura *screened subnet* é um melhoramento da arquitetura *screened host*, pois adiciona uma camada extra de segurança que isola a rede interna de uma rede externa não confiável. Essa camada é chamada DMZ e possui três elementos, sendo estes dois roteadores e um *bastion host*. No modelo *screened host* se o *bastion host* fosse comprometido o invasor teria total acesso a rede interna, isso não ocorre na arquitetura *screened subnet*. O *bastion* host fica na DMZ e caso ele seja comprometido, o filtro interno ainda protegerá a rede interna. De acordo com NAKAMURA e GEUS (2007) o filtro externo deve permitir o acesso externo aos serviços que estão na DMZ, assim como as requisições dos usuários internos.

Vale ressaltar que as arquiteturas apresentadas são as mais comumente utilizadas, porém não são regras, elas servem apenas como orientação e referencia teórica, não existindo uma arquitetura única, a qual irá resolver todos os problemas de segurança.

3 APRESENTAÇÃO E ANÁLISE DOS RESULTADOS

3.1 CHECK POINT

A Check Point foi fundada em 1993 por Gil Shwed e foi uma das primeiras empresas no setor de segurança de TI comercializando o primeiro *Firewall e também o* criador da tecnologia *Stateful Firewall,* que foi patenteada, ele analisa o tráfego a partir da tabela de estados de conexões legítimas, e que até hoje embasa a maioria das tecnologias de segurança de rede.

O foco da Check Point sempre foi atender as necessidades dos seus clientes afim de garantir a segurança nas transações e comunicação através do uso da Internet pelas corporações e em busca de uma arquitetura unificadas de segurança em 2006 a Check Point criou um único console o gerenciamento, *gateways* de segurança unificados e o primeiro agente único para segurança de *endpoints*. No início de 2009 introduziu o *Software Blade*, uma arquitetura dinâmica e personalizada que visava oferecer soluções seguras, flexíveis e simples para atender às necessidades das organizações.

Ainda em 2009 a empresa concluiu a aquisição de *appliances* de segurança da Nokia e adquiriu o banco de dados de aplicativos da *Face Time Communications*, dessa maneira a Check Point conseguiu adicionar controles de segurança para mais de 50.000 *widgets* da *Web* 2.0 e mais de 4.500 aplicativos da Internet aos *gateways* de segurança.

Atualmente a Check Point possui 20,6% segundo a do mercado mundial de *firewall,* sendo elencada como líder no quadrante mágico de Gartner[3] figura 7, e sendo reconhecida como líder mundial deste mercado.

---

[3]Gartner – É uma empresa de consultoria fundada em 1979 por Gideon Gartner. A Gartner desenvolve tecnologias relacionadas a introspecção necessária para seus clientes tomarem suas decisões todos os dias.
Fonte:<https://www.opservices.com.br/o-que-e-o-quadrante-magico-do-gartner.html> acessado em 17/05/2017.

Figura 7 - lustração do Quadrante Mágico do Gartner
Fonte: <https://br.pinterest.com/pin/571323902708660325/>Acesso em: 19 agosto. 2016.

A Check Point continua inovando e desenvolvendo o *Software Blade Architecture* e visa definir a segurança como um processo de negócios através do Check Point 3D *Security* que visa combinar de forma única a política, as pessoas e a fiscalização para uma maior proteção dos recursos de informação e ajuda as organizações a implementar um plano de segurança que alinha as necessidades do negócio.

Como clientes podemos citar todas as empresas Fortune e Global 100, e suas soluções continuam em destaque como as premiadas soluções ZoneAlarm que protege milhões de consumidores contra *hackers*, *spyware* e roubo de dados.

3.1.1 **Stateful *Firewall***

O *firewall* baseado em pacotes, que surgiu na década de 80 antes da tecnologia *Stateful Firewall* , analisava o cabeçalho dos pacotes e este era liberado conforme as regras pré-estabelecidas e adicionalmente o *firewall* pode realizar alguma outra atividade, como um registro de acesso, ou outra determinação estabelecida. Neste tipo de *firewall* a análise é baseada nas camadas de rede e transporte do modelo TCP/IP. Este *firewall* acaba por não realizando nenhum tipo de decodificação do protocolo ou analisando a camada de aplicação.

A tecnologia Stateful *Firewall* desenvolvido pela Check Point tem por objetivo averiguar a conformidade dos dados com as regras, reconhecendo no tráfego para qual porta o pacote deve ser direcionado, não permitindo que o tráfego seja direcionado a outro destino que não o que esteja definido em seu cabeçalho. Ela é capaz de identificar o protocolo dos pacotes transitados e faz uma espécie de comparação entre o que está acontecendo e o que é esperado para acontecer, prevendo assim respostas legítimas. Para que isso ocorra o *firewall* analisa todo o tráfego de dados em busca de padrões aceitáveis que continuaram sendo utilizados para manter a comunicação.

Com o tempo surgiu a necessidade da análise e checagem de todas as 7 camadas do modelo OSI e foram surgindo aperfeiçoamentos como o *Deep Packet Inspection,* ou SMLI (*Stateful Multi-Layer Inspection*). Esta tecnologia visa decodificar o pacote para poder interpretar o tráfego do ponto de vista cliente/servidor, além de incluir algumas técnicas específicas de identificação de ataques e simultaneamente analisa o tráfego a partir da tabela de estados de conexões legítimas para comparar os pacotes com padrões legítimos de tráfego visando identificar possíveis anomalias ou ataques. A combinação dessas duas análises permite que novos padrões sejam reconhecidos e adicionados às regras válidas.

Com o tempo foi necessário desenvolver um novo método que fosse capaz de analisar as particularidades de cada protocolo e tomar decisões específicas que pudessem evitar ataques maliciosos contra uma rede.

3.1.2 **DLP – *Data Loss Prevention***

A solução de DLP (*Data Loss Prevention*) visa evitar vazamentos de dados não intencionais por intermédio da identificação, monitoramento e proteção da transferência de dados através de uma profunda verificação dos conteúdos e análise de parâmetros de transação (como origem, destino, objeto de dados e protocolo), por meio de uma estrutura de gerenciamento centralizada. Em resumo, o DLP detecta e impede a transmissão não autorizada de informações confidenciais.

O Check Point DLP possui uma tecnologia inovadora que fornece automação e anula a necessidade de análise longa e dispendiosa, passando de uma política de detecção única para uma política de prevenção precisa e eficaz. A funcionalidade DLP Check Point possui uma fácil interface a qual pode ser personalizada.

O DLP da Ckeck Point possui também um *Software* Blade que possui um grande número de tipos de dados internos que podem ser rapidamente aplicados como uma política padrão. Políticas *out-of-the-box* podem converter facilmente as diretrizes de confidencialidade e integridade da organização em regras automatizada, e mais tarde, pode criar os próprios tipos de dados. Este ciclo de atualização da política, passando de uma política de detecção para uma política preventiva.

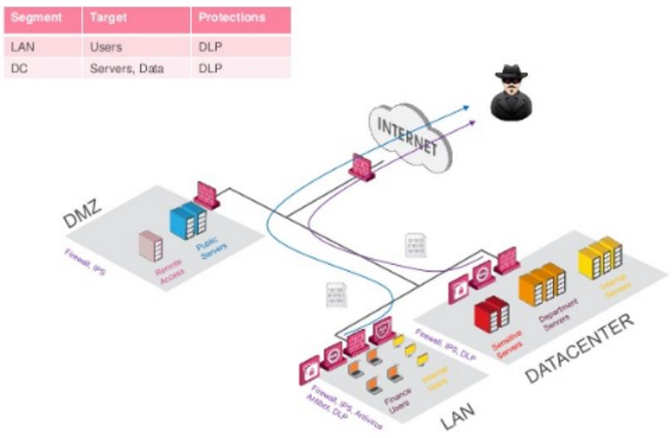


Figura 8 - Detecta e Impede a Transmissão não Autorizada.
Fonte: <https://www.checkpoint.com/products/dlp-software-blade/>
Acesso em 10 de junho de 2017.

3.1.3 **SandBlast**

A Check Point SandBlast oferece proteção abrangente contra até mesmo os ataques mais perigosos, garantindo simultaneamente a entrega rápida de conteúdo seguro para os usuários. No núcleo da solução estão duas capacidades únicas:

a) Emulação de ameaças e extração de ameaças que levam a defesa de ameaças para o próximo nível.

Como parte da solução Check Point SandBlast, o mecanismo de emulação de ameaças detecta *malware* na fase de exploração, mesmo antes que hackers possam aplicar técnicas de evasão. Os arquivos são rapidamente colocados em quarentena e inspecionados, rodando em uma caixa de proteção virtual para detectar comportamentos mal-intencionados antes de entrar na rede. Esta solução inovadora combina a inspeção no nível da CPU e o sandboxing no nível do sistema operacional para evitar a infecção perigosas e ataques direcionados.

Além disso, o recurso SandBlast *Threat Extraction* fornece imediatamente uma versão segura de conteúdo potencialmente mal-intencionado para os usuários. Conteúdo explorável, incluindo conteúdo ativo e várias formas de objetos incorporados, são extraídos do arquivo *econstructed* para eliminar ameaças potenciais. O acesso à versão suspeita original é bloqueado, até que possa ser totalmente analisado pela SandBlast Zero-*Day Protection*. Os usuários têm acesso imediato ao conteúdo e podem estar confiantes de que estão protegidos contra as ameaças mais avançadas de *malware* .

3.1.4 **Security check-up**

A Check Point oferece um relatório identificado como *Security Check-Up* no qual identifica os riscos da rede fornecendo uma análise das ameaças e apresenta todos os incidentes de segurança detectados como os acessos a aplicações *web* de alto risco, computadores infectados com *malware*, vulnerabilidades e ataques, incidentes de fuga de dados e apresenta quais as recomendações para a proteção da rede.

A avaliação do Security Checkup implanta um gateway de segurança Check Point dentro da rede, inspecionando o tráfego que atravessa a rede. O *gateway* não está conectado *in-line*, evitando alterações de configuração de rede e tempo de inatividade. Em vez disso, ele inspeciona o tráfego de rede espelhado usando a *Monitor Port* conectada a um dispositivo TAP (*Test Access Point*) ou uma *Mirror Port* (também conhecida como *Span Port*) em um comutador de rede. Ao fazê-lo, remove todos os desafios da conectividade *in-line*, garantindo a inspeção apenas do tráfego de rede copiado. Como a *Monitor Port* não transmite nenhum tráfego para a rede, não há alteração na configuração de rede existente e nenhum risco de indisponibilidade.

Qualquer organização pode participar de um *Security Ckeck-Up*, independentemente de estarem usando soluções Check Point ou não. Os especialistas em segurança realizam avaliações no local que incluem quatro etapas principais:

3.1.4.1 Check Point *Security Gateway Setup*

O especialista em segurança configura o Check Point *Security Gateway* no qual a avaliação será realizada. A seguir, ativam e configuram todas as lâminas relevantes do Check Point *Software*. Estes podem incluir Controle de Aplicativos, Filtragem de URLs, IPS, Anti-Bot, AntiVirus, Emulação de Ameaça, DLP, Consciência de Identidade, se necessário, SmartEvent ou mais.

- **Inspeciona o tráfego da rede -** O dispositivo chega no local. Uma vez conectado à rede da organização, ele começa a inspecionar o tráfego da rede. Para garantir uma inspeção completa, que ocorre por pelo menos uma semana, porém quanto mais tempo o período de inspeção, melhor.
- **Análise de Resultados -** Depois de remover o dispositivo da rede, o especialista em segurança analisa os resultados e gera o relatório de Verificação de Segurança.

- **Relatório de Resultados -** O especialista em segurança apresentará os resultados que identificam pontos fracos na rede. Em seguida, é apresentado as tecnologias de segurança e soluções recomendadas.

O *Security Check-Up* visa uma maior conscientização da exposição ao risco de segurança, identificação e priorização de lacunas de segurança que exigem melhorias e introdução à tecnologia de segurança mais recente que abrange todos os aspectos da segurança da rede.

3.1.5 **ESTUDO DE CASO**

Em seguida será apresentado um exemplo prático do *Security Check-Up* aplicado em uma cooperativa do estado do Paraná presente no mercado brasileiro de alimentos há mais de 35 anos.

O relatório de verificação de segurança a seguir apresenta os resultados de uma avaliação de segurança realizada na rede. O relatório descobre onde a organização está exposta a ameaças de segurança e oferece recomendações para lidar com esses riscos.

Para se destacar, o tráfego de rede foi inspecionado pelo Check Point para detectar uma variedade de ameaças de segurança, incluindo: infecções por *malware*, aplicações *web* de alto risco, tentativas de intrusões, perda de segurança dados e muito mais.

A Figura 9 apresenta a visão geral da análise e em seguida descrevemos item a item na análise, como pode ser observado na figura 9 há 15 computadores com infectados com BOTs e 12 computares suscetíveis a invasão.

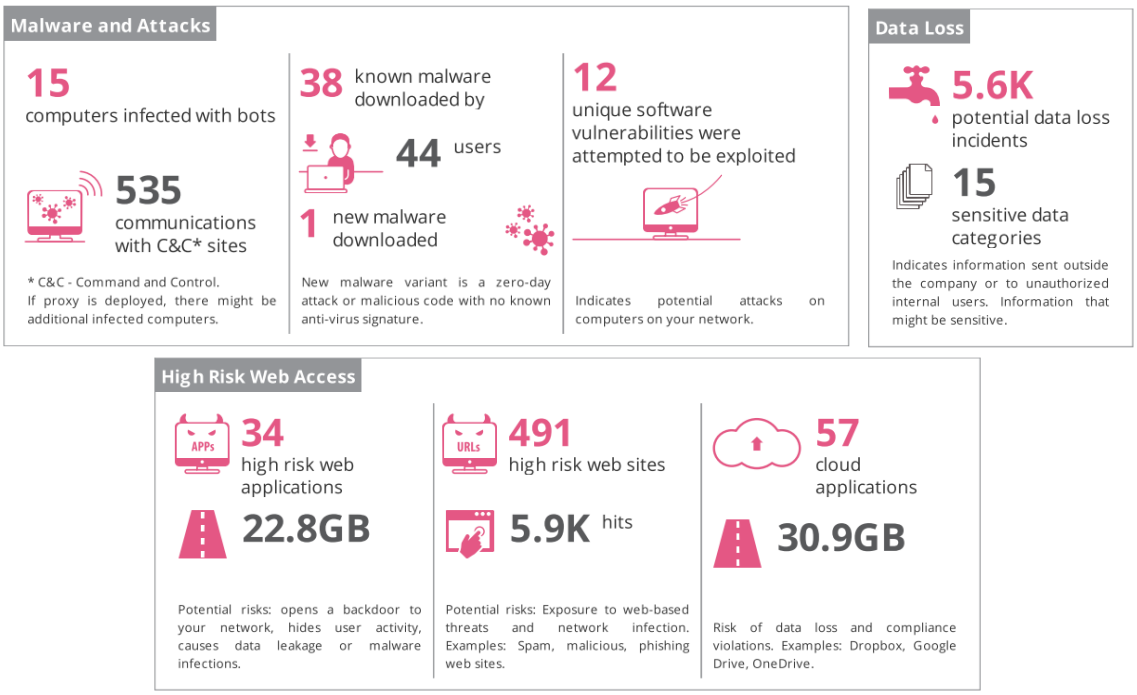


Figura 9 - Resultados Utilisando o *Software* Check Point.
Fonte: Autores

3.1.5.1 Máquinas Infectadas com BOTs

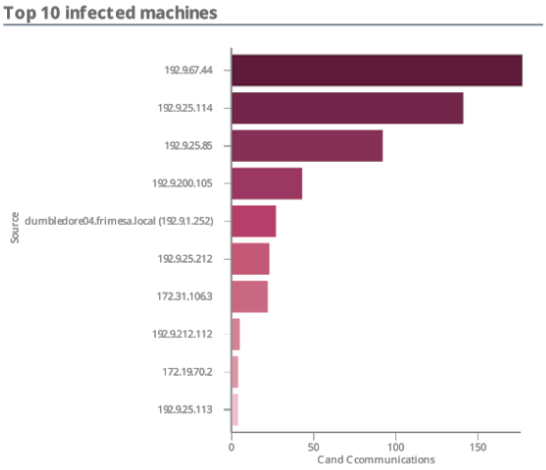
Um Bot é um *software* malicioso que invade o seu computador. Os BOTs permitem que os criminosos controlem remotamente o seu computador para executar atividades ilegais, como por exemplo, transmitir dados, fazer propaganda de *malware* e participar de ataques de Negação de Serviço (DOS) sem o seu conhecimento. Os BOTs desempenham um papel chave em ataques direcionados conhecidos como *Advanced Persistent Threats* (APTs); A tabela 1 mostra as famílias de BOT e o número de computadores infectados detectados na rede.

Tabela 1 - Famílias de BOT e o Número de Computadores Infectados.

(continua)

Bot infections (top 20 bots)

Malware Name*	Malware Family	Infected Computers**	Destination Country
Operator.Iniduoh.d	Iniduoh	192.9.67.44	
		192.9.25.114	
		192.9.25.85	
		192.9.25.212	
		192.9.25.113	
		Total: 5 Computers	**0 Countries**
Worm.Win32.Iniduoh.A	Iniduoh	192.9.67.44	
		192.9.25.114	
		192.9.25.85	
		192.9.25.212	
		192.9.25.113	
		Total: 5 Computers	**0 Countries**



Fonte: Autores.

Tabela 1 - Famílias de BOT e o Número de Computadores Infectados.

(conclusão)

Malware Name*	Malware Family	Infected Computers**	Destination Country
Operator.Iniduoh.f	Iniduoh	192.9.25.85	
		192.9.25.212	
		192.9.25.113	
		Total: 5 Computers	**0 Countries**
Operator.Iniduoh.e	Iniduoh	192.9.67.44	
		192.9.25.114	
		192.9.25.85	
		192.9.25.212	
		Total: 4 Computers	**0 Countries**
Operator.Conficker_C.easeb	Conficker_c	192.9.19.45	Brazil
		dumbledore04.frimesa.local (192.9.1.252)	United States
		192.9.200.105	United States
		Total: 3 Computers	**2 Countries**
Operator.cnc server.bgrm	Cnc server	192.9.212.112	United States
		192.9.1.16	
		192.9.200.105	United States
		Total: 3 Computers	**1 Country**
Operator.Cryptodef.chm	Cryptodef	192.9.1.16	
		192.9.200.105	United States
		192.9.212.112	
		Total: 3 Computers	**1 Country**
Operator.cnc server.cfu	Cnc server	172.31.106.3	Luxembourg Netherlands Russian Federation
Operator.cnc server.cfu	Cnc server	192.9.200.105	United States
		Total: 2 Computers	**4 Countries**
Operator.Ponmocup.bq	Ponmocup	172.19.70.2	
		192.9.200.105	United States
		Total: 2 Computers	**1 Country**
Operator.Ponmocup.bn	Ponmocup	172.19.70.2	
		192.9.200.105	United States
		Total: 2 Computers	**1 Country**
Operator.Ponmocup.m	Ponmocup	172.19.70.2	
		192.9.200.105	United States
		Total: 2 Computers	**1 Country**
Operator.cnc server.bmkx	Cnc server	192.9.200.105	United States
		192.9.50.118	Netherlands
		Total: 2 Computers	**2 Countries**
Phishing.cujazy		172.31.106.3	United States
		192.9.212.112	United States
		Total: 2 Computers	**1 Country**
REP.hssmmu		192.9.200.105	United States
		Total: 1 Computer	**1 Country**
phishing.dcac		192.9.200.105	United States
		Total: 1 Computer	**1 Country**
Phishing.czbukp		dumbledore04.frimesa.local (192.9.1.252)	United States
		Total: 1 Computer	**1 Country**
Malware.yqxgg		dumbledore04.frimesa.local (192.9.1.252)	Brazil
		Total: 1 Computer	**1 Country**
phishing.dbyz		172.31.106.3	United States
		Total: 1 Computer	**1 Country**
REP.uikik		192.9.200.105	Canada
		Total: 1 Computer	**1 Country**
Phishing.cyxmbq		dumbledore04.frimesa.local (192.9.1.252)	United States
		Total: 1 Computer	**1 Country**
Total: 39 Malware	**6 Families**	**15 Computers**	**9 Countries**

Fonte: Autores

3.1.5.2 Máquinas Infectadas com *Adware* e *Toolbars*

Adware e barras de ferramentas são programas potencialmente indesejados projetados para exibir anúncios, redirecionar solicitações de pesquisa para s*ites* de publicidade e coletar dados do tipo de *marketing* sobre o usuário para exibir publicidade personalizada no computador. Computadores infectados com esses programas devem ser diagnosticados como eles podem ser expostos a infecção de acompanhamento de um *malware* de alto risco. A tabela 3 a seguir resume as famílias de *malware,* de *adware,* barra de ferramentas e o número de computadores infectados detectados na rede.

Tabela 2 - Famílias de *Malware* de *Adware*

Adware Name*	Infected Computers**
Operator.Generic.dgf	5 Computers
Adware.Win32.Casalemedia.N	1 Computer
Adware.Win32.Domaiq.P	1 Computer
Total: 3 Adware	**6 Computers**

Fonte: Autores

3.1.5.3 Malware Downloads (Malware Conhecido)

Com a crescente incidência de ameaças cibernéticas, muitos ataques direcionados começam com a exploração de vulnerabilidades de *software* em arquivos baixados e anexos de *e-mail*. Durante a análise de segurança, uma série de eventos relacionados a *malware* que indicam *downloads* de arquivos maliciosos foram detectados. Os gráfico 2 mostra os computadores infectados por arquivos de *malware* conhecidos, eles foram detectados na rede e o número de computadores que fizeram o *download*. Os *malware*s conhecidos, referem-se a *malware* para o qual existem assinaturas, e portanto, devem ser bloqueados por um sistema antivírus. O no gráfico 3 demonstra a origem dos *malware.*

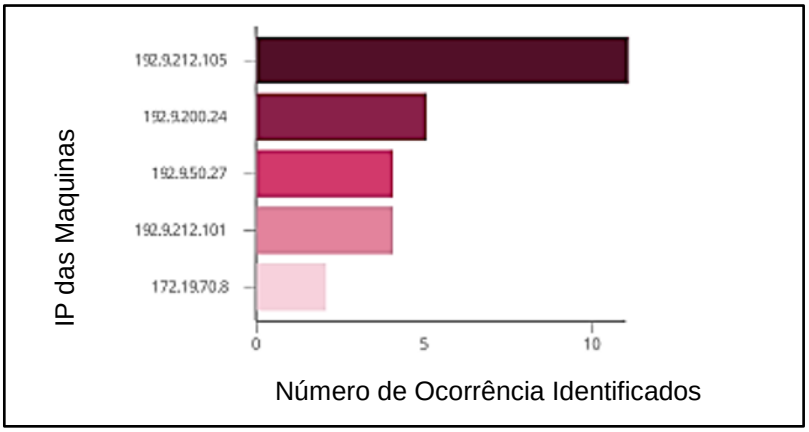


Gráfico 2 - Endereço IP das Ocorrências de *Malware*
Fonte: Autores

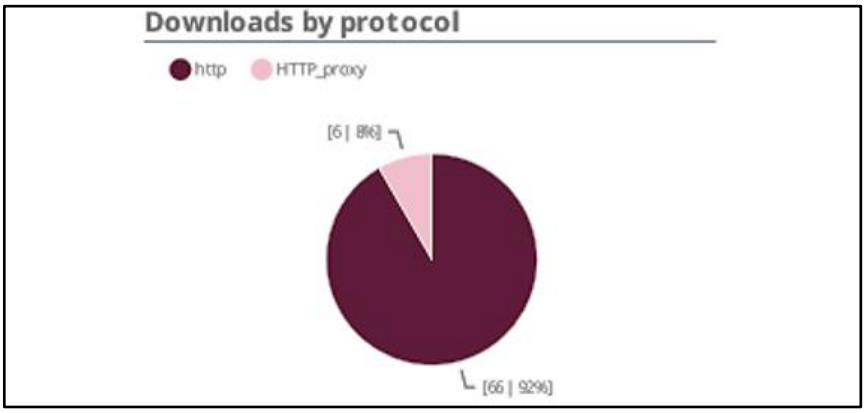


Gráfico 3 - Origens dos *Downloasds* queTiveram Ocorrência de *Malware*.
Fonte: Autores

3.1.5.4 Transferências de Variants *Malware* Novos (*Malware Unknown*)

Com as ameaças *cyber* tornando-se cada vez mais sofisticados, ameaças avançadas muitas vezes incluem novas variantes de *malware* sem proteções existentes, conhecido como "*malware* desconhecido". A tabela 4 resume d*ownloads* de novas variantes de *malware* detectadas na rede. Essas ameaças incluem novas explorações (zero dia) ou mesmo variantes de explorações conhecidas, sem assinaturas existentes, e portanto, não são detectáveis por soluções padrão o gráfico 4 demonstra a quantidade de *malware* desconhecidos. A detecção desses tipos de *malware* requer que sejam executados em uma caixa de proteção virtual para detectar comportamentos mal-intencionados. Durante a análise de segurança, uma série de eventos relacionados a *malware* foram detectados na sua rede.

Tabela 3 - Novas Variantes de *Malware* Detectadas na Rede.

177.6K Total files scanned

1 Total malware found (using sandboxing technology)

Downloads of new malware variants (top 20)

Infected File Name	Source	Malicious Activities	Downloa...	MD5*	Protocol
NBR-8.160-Sistemas-Prediais-de-Esgoto-Sanitrio-Projeto-e-Execuo.pdf	172.31.106.3 192.9.25.155	Malware signature matched (Trojan.Win32.Generic.T.loxo)	4	a7b1c7df8c6d478c3f45cb011848930c	HTTP_proxy http
Total: 1 File	**2 Sources**	**1 Malicious activity**	**4**	**1 MD5**	**2 Services**

Fonte: Autores

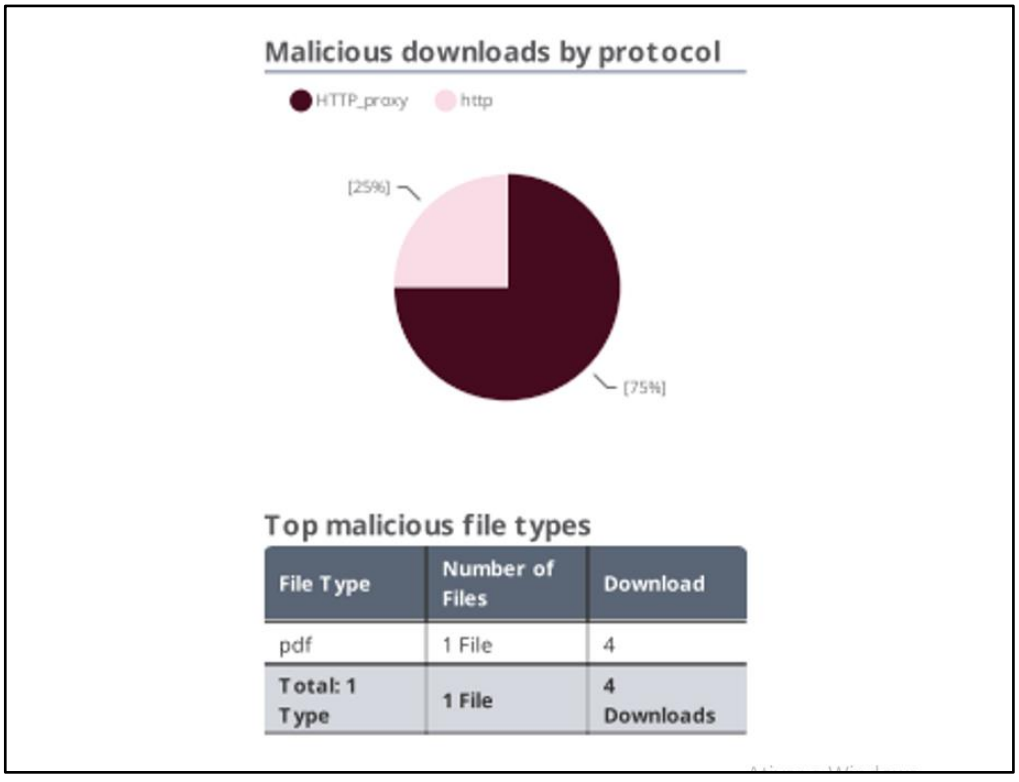


Gráfico 4 - Ocorrência de "*Malware* Desconhecido".
Fonte: Autores

3.1.5.5 Acesso a *Sites* Conhecidos para Conter *Malware*

As organizações podem ficar infectadas com *malware* acessando *Sites* mal-intencionados durante a navegação na Internet ou clicando em *links* maliciosos incorporados no e-mail recebido. A tabela 5 é são eventos relacionados a *Sites* conhecidos por conterem *malware*, e o gráfico 5 mostra os IPs e o número de acesso que realizaram a esse *site*.

Tabela 4 - Sites Conhecidos por Conterem *Malware*

URL	Hits
http://maroco.linkpc.net/is-rinoy	116
http://maroco.linkpc.net/is-rinoy	115
http://maroco.redirectme.net/is-rinoy	106
http://maroco.redirectme.net/is-rinoy	105
http://maroco.myq-see.com/is-rinoy	104
http://maroco.myq-see.com/is-rinoy	104
	47
http://daatspaper.com/index/xwyqw.inf	36
http://serverpost.club/server.htm	22
http://74.207.251.31/br/flashplayer/	17
	944

Fonte: Autores

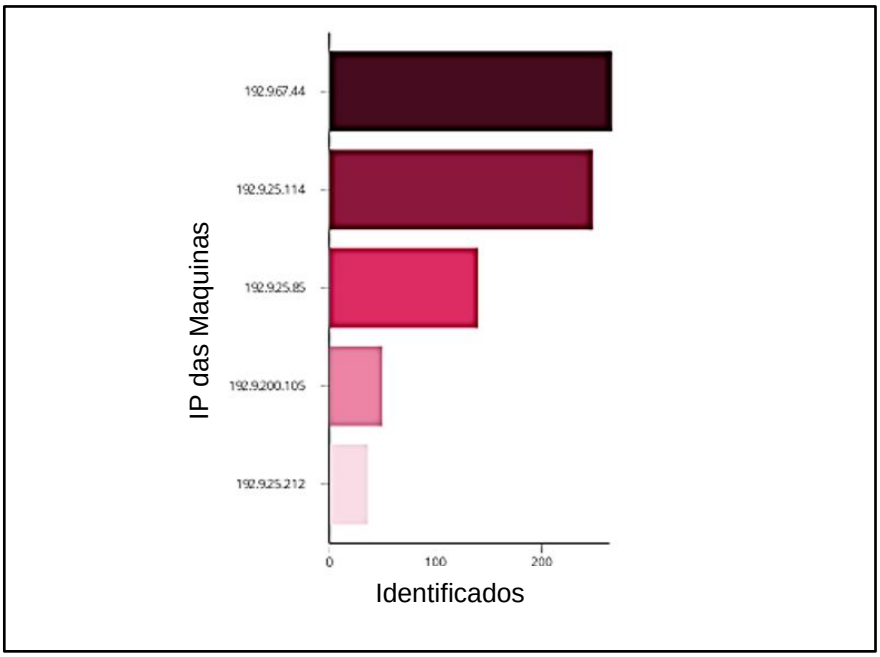


Gráfico 5 - Os Cinco Endereços IP com Maior Número de Ocorrência de *Malware*.
Fonte: Autores

3.1.5.6 Ataques e Vulnerabilidades do *Software* Explorado

Durante a análise de segurança, os ataques e vulnerabilidades de *software* explorado em servidores/clientes foram detectados. Tais incidentes podem indicar tentativas de intrusão, ataques de *malware* , ataques DOS ou tentativas de transpor a segurança explorando vulnerabilidades de *software*. O APÊNDICE A resume esses eventos evidenciando os *softwares* vulneráveis.

3.1.5.7 Utilização de Aplicações *Web* de Alto Risco

As aplicações *Web* são essenciais à produtividade de cada organização, mas também criam graus de vulnerabilidade na sua postura de segurança. Os aplicativos de administração remota podem ser legítimos quando usados pelos administradores e pelo *help-desk*, mas observe que algumas ferramentas de acesso remoto também podem ser usadas para ataques cibernéticos. As aplicações *web* de risco que foram detectadas na rede foram ordenadas por categoria, nível de risco e número de utilizadores, ver o APÊNDICE B a lista com as 10 aplicações *web* de alto risco encontradas nesta analise, abaixo o grafítico 6 evidenciando quais maquinas mais utilizaram esse serviço.

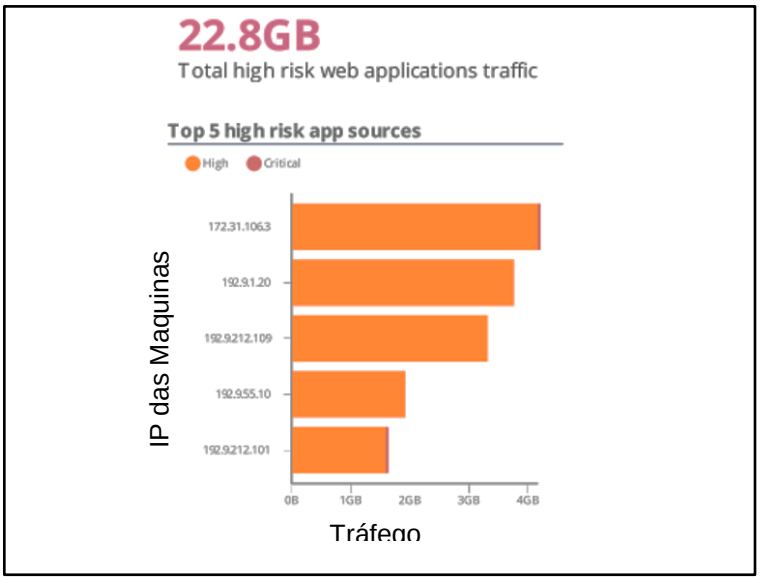


Gráfico 6 - Os Cinco Endereços IP com maior Tráfego.
Fonte: Autores

3.1.5.8 Acesso à *Web Sites* de Alto Risco

O uso da *Web* é onipresente nos negócios de hoje. Mas a natureza dinâmica e em constante evolução da *web* torna extremamente difícil proteger e reforçar o uso da *web* em um ambiente corporativo. Para tornar as coisas mais complicadas, o tráfego da *Web* evoluiu para incluir não apenas o tráfego de URLs, mas também os URLs e aplicativos incorporados. A identificação de locais de risco é mais crítica do que nunca. Os acessos aos seguintes *Sites* de risco foram detectados na rede, organizados por categoria, número de utilizadores e número de acessos a tabela 6 tem-se os acessos a sites de alto risco.

Tabela 5 - Aplicações *Web* de Alto Risco.

Website Category	Hits
	5.9K
Total: 0 Categories	**5.9K Hits**

Top high risk web sites (top 10 per category)

Site Category	Site	Users	Hits
	178.255.154.51 184.106.197.231/.promo2016/imgexedoc.png 2dayconsultoria.com.br 2dh.com.br 2ktrack3.com 37.48.71.22 37.48.71.26 3jsbf5.xyz 4lmbkpqrklqv.net/js/analytic.php 99widgets.com 481 more Sites	10.250.66.10 172.19.65.3 172.19.65.4 172.19.66.1 172.19.67.1 549 more Users	5.9K
Total: 0 Categories	**491 Sites**	**554 Users**	**5.9K**

Fonte: Autores

3.1.5.9 Incidentes de Perdas de Dados

Os dados internos de sua empresa são um dos seus mais valiosos conjuntos. Quaisquer danos intencionais ou não intencionais podem causar danos à sua organização. As informações da tabela 7 foram enviadas para fora da empresa ou para usuários internos potencialmente não autorizados. Estas informações podem potencialmente ser informações sensíveis que devem ser protegidas contra perda. O seguinte representa as características dos eventos de perda de dados que

foram identificados durante o curso da análise, na tabela 7 demonstra o número de arquivos e protocolos analisados, e na tabela 8 as aplicações web utilizadas.

Tabela 6 - Incidentes de Envios de Dados.

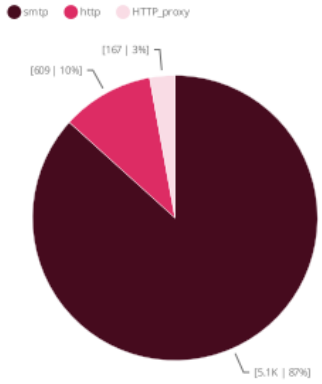
Summary

278.7K Total emails scanned **5.1K** Emails with data loss incidents **585** Web data loss incidents

Data loss incidents by data types (top 20)

Data Type	Users	Events	Service
PCI - Cardholder Data	dumbledore04.frimesa.local (192.9.1.252)	4.7K	smtp
	192.9.25.196	101	HTTP_proxy http
	192.9.25.175	57	HTTP_proxy http
	192.9.25.210	34	HTTP_proxy http
	192.9.50.135	28	http
	Total: 116 Users	**5.4K**	**3 Services**
Internal Users and a New External Recipient	dumbledore04.frimesa.local (192.9.1.252)	72	smtp
	Total: 1 User	**72**	**1 Service**
U.S. Social Security Numbers - According to SSA	172.19.186.4	9	http
	dumbledore04.frimesa.local (192.9.1.252)	6	smtp
	192.9.68.8	4	http
	172.20.96.5	3	http
	172.20.112.4	3	http

Incidents by protocol



Fonte: Autores

Tabela 7 - Aplicações *Web* Utilizadas para os Envios.

Cloud based web applications (top 20)

Application Name	Traffic Total Bytes	Application Category	Users
SharePoint-online	11.6GB	Business Applications	8 Users
Dropbox	6.6GB	File Storage and Sharing	55 Users
Google Analytics	3.1GB	Business Applications	663 Users
SourceForge	1.5GB	Web Services Provider	18 Users
Google Cloud Storage	1.2GB	File Storage and Sharing	136 Users
Adobe Creative Cloud	1.2GB	Business Applications	8 Users
Google Drive-web	1003.4MB	File Storage and Sharing	59 Users
MediaFire-web-download	827.1MB	File Storage and Sharing	14 Users
Office365-Outlook-web	681.7MB	Email	53 Users
Zippyshare-Download	495.8MB	File Storage and Sharing	8 Users
iCloud	439.7MB	Media Sharing	20 Users
Office365	383.0MB	Business Applications	80 Users
pCloud	313.6MB	File Storage and Sharing	3 Users
ImageBam	299.3MB	Media Sharing	18 Users
Adobe Connect	266.4MB	Web Conferencing	111 Users
Mega	232.8MB	File Storage and Sharing	13 Users
SoundCloud	215.7MB	Media Sharing	45 Users
Google Cloud Storage-download	153.6MB	File Storage and Sharing	275 Users
Google App Engine	91.4MB	Web Services Provider	157 Users
MediaFire	82.2MB	File Storage and Sharing	24 Users
Total: 57 Applications	**30.9GB**	**11 Categories**	**764 Users**

Fonte: Autores

3.1.5.10 Utilização de Banda Larga por Aplicações & *Web* Sites

A largura de banda da rede da organização é normalmente utilizada por uma ampla gama de aplicações *web* e s*ites* usados pelos funcionários. Aplicativos que usam muita largura de banda, por exemplo, mídia de fluxo contínuo, podem limitar a largura de banda que está disponível para aplicativos de negócios importantes. É importante entender o que está acumulando a largura de banda da rede, a fim de limitar o consumo de largura de banda de uso não relacionado a negócios. O seguinte resume listado na tabela 9, mostra a utilização da largura de banda da sua organização ordenada por largura de banda consumida.

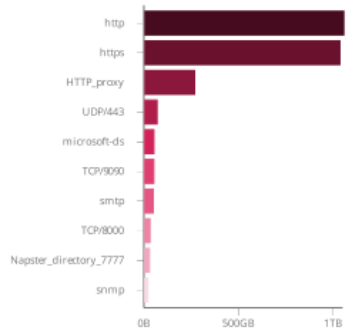
Tabela 8 - Utilização e Consumo da Banda por Aplicações & *Web Sites*.

Top applications/sites (top 30)

Application / Site	Category	Risk Level	Sources	Traffic
Google Services	Computers / Internet	2 Low	885 Sources	233.9GB
YouTube	Media Streams	2 Low	390 Sources	157.5GB
Facebook	Social Networking	2 Low	339 Sources	129.2GB
Windows Update	Software Update	1 Very Low	645 Sources	99.5GB
SSL Protocol	Network Protocols	1 Very Low	497 Sources	62.3GB
Quic Protocol	Network Protocols	2 Low	39 Sources	54.9GB
SMTP Protocol	Network Protocols	3 Medium	61 Sources	40.0GB
SHOUTcast	Media Sharing	2 Low	63 Sources	22.8GB
Skype	VoIP	3 Medium	122 Sources	22.7GB
Server Message Block (SMB)-write	Network Protocols	1 Very Low	146 Sources	21.7GB
Google Play	Search Engines / Portals	2 Low	62 Sources	21.2GB
Trend Micro Active Update	Software Update	1 Very Low	2 Sources	17.2GB
Server Message Block (SMB)	Network Protocols	1 Very Low	381 Sources	16.6GB
HTTP/2 over TLS	Network Protocols	1 Very Low	336 Sources	16.4GB
Vevo	Media Sharing	2 Low	13 Sources	15.8GB

2.5TB
Total traffic scanned

Traffic by protocol

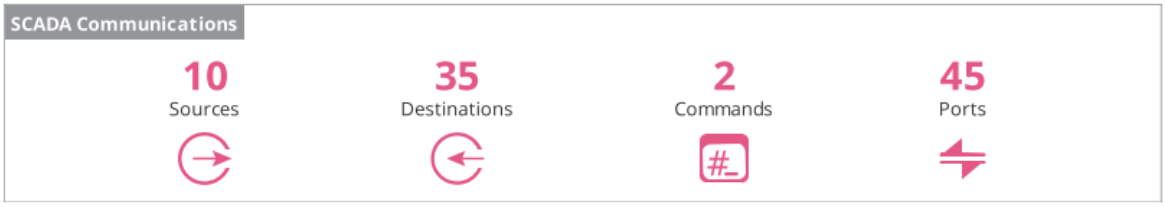


Application / Site	Category	Risk Level	Sources	Traffic
Java Remote Method Protocol	Network Protocols	2 Low	100 Sources	15.7GB
WhatsApp Messenger-file transfer	Media Sharing	3 Medium	20 Sources	13.9GB
SNMP Protocol	Network Protocols	2 Low	38 Sources	13.2GB
SharePoint-online	Business Applications	1 Very Low	8 Sources	11.6GB
DNS Protocol	Network Protocols	1 Very Low	581 Sources	9.5GB
Apple Software Update	Software Update	1 Very Low	10 Sources	8.6GB
WhatsApp Messenger	Instant Messaging	2 Low	17 Sources	8.2GB
WeTransfer	File Storage and Sharing	3 Medium	13 Sources	7.4GB
Google Maps-web api	Vehicles	2 Low	629 Sources	7.0GB
Dropbox	File Storage and Sharing	4 High	55 Sources	6.6GB
VNC-clipboard	Remote Administration	3 Medium	37 Sources	6.4GB
App Store	Search Engines / Portals	1 Very Low	10 Sources	6.3GB
BitTorrent Protocol	P2P File Sharing	4 High	7 Sources	5.8GB
Office on Demand	Business Applications	2 Low	29 Sources	5.3GB
MSN-web	Search Engines / Portals	2 Low	369 Sources	5.1GB
Total: 643 Applications / Sites	**47 Categories**	**6 Risks**	**1416 Sources**	**1.2TB**

Fonte: Autores

3.1.5.11 Protocolo SCADA

SCADA (*Supervisory Control and Data Acquisition*) é um tipo de sistema de controle industrial (ICS) que monitora e controla processos industriais. Ele opera com sinais codificados através de canais de comunicação, de modo a fornecer controle de equipamentos remotos. As redes SCADA são normalmente separadas da rede de TI organizacional para fins de segurança. Os protocolos SCADA detectados na rede de TI podem indicar um risco de segurança com potencial para uma violação de segurança. Na figura 10 um exemplo protocolos SCADA, foram detectados na rede na desta empresa duas aplicações DNP3 e EtherNet/IP.



Top SCADA commands (top 20)

Protocol & Command	Transactions	Traffic
DNP3 Protocol	50	0B
EtherNet/IP	9	2.9MB
Total: 2 Protocols & Commands	**59 Transactions**	**2.9MB**

Figura 10 - Exemplo de Monitoramento em Redes Industriais
Fonte: Autores

3.2 PROTEÇÃO DEFINIDA POR *SOFTWARE*

Proteção definida por *software* é uma nova arquitetura e metodologia de segurança pragmática. Ele oferece uma infraestrutura que é modular, ágil e mais importante, segura. Essa arquitetura deve proteger organizações de todos os tamanhos em qualquer local: redes de matrizes, filiais, *roaming* através de *smartphones* ou dispositivos móveis ou ao usar ambientes de nuvem.

As proteções devem se adaptar automaticamente à paisagem de ameaças sem a necessidade de administradores de segurança acompanharem manualmente

milhares de recomendações e recomendações. Essas proteções devem integrar-se perfeitamente em um ambiente de TI maior e a arquitetura deve fornecer uma postura defensiva que colaborativamente alavanca fontes internas e externas inteligentes.

A arquitetura de Proteção Definida por *Software* (SDP) divide a infraestrutura de segurança em três camadas interconectadas:

- Uma Camada de Aplicação que é baseada em pontos de aplicação de segurança física, virtual e baseada em host e que segmentos da rede, bem como executa a lógica de proteção em ambientes de alta demanda.
- Uma Camada de Controle que analisa diferentes fontes de informações sobre ameaças e gera proteções e políticas a serem executadas pela camada de aplicação.
- Uma Camada de Gerenciamento que orquestra a infraestrutura e traz o grau de agilidade de toda a arquitetura.

Ao combinar a Camada de Aplicação de alto desempenho com a Camada de Controle baseada em *software* dinâmico e de rápida evolução, a arquitetura SDP fornece não apenas resiliência operacional, mas também prevenção proativa de incidentes para uma paisagem de ameaças em constante mudança.

Projetada para ser voltada para o futuro, a arquitetura SDP, figura esquema suporta os requisitos tradicionais de segurança de rede e políticas de controle de acesso, bem como a prevenção de ameaças exigida pelas modernas empresas que adotam novas tecnologias, como computação móvel e redes definidas por *software* (SDN).

3.2.1 ***Software* Check Point**

A Check Point fornece todos os componentes certos necessários para implementar uma arquitetura SDP completa com o melhor gerenciamento e a melhor segurança.

As proteções definidas pelo *software* Check Point fornecem a flexibilidade necessária para lidar com novas ameaças e abraçar novas tecnologias. Nossas soluções geram proteções novas e atualizadas para ameaças conhecidas e desconhecidas e pro-ativamente distribuem esse conhecimento através da nuvem. A implementação de soluções de segurança Check Point baseadas em design de segurança de arquitetura sonora capacita as empresas a adotar soluções de sistemas de informações de ponta com confiança.

3.2.2 **Check Point SDP *Enforcement Layer***

Para garantir os limites de cada segmento, a Check Point oferece uma ampla gama de pontos de aplicação. Estes incluem dispositivos de segurança de rede de alto desempenho, *gateways* virtuais, *software* de host de ponto final e aplicativos de dispositivo móvel (Check Point *Capsule*), que permite estender a segurança da rede corporativa e aplicá-la aos seus dispositivos móveis. A Check Point fornece todos os blocos de construção necessários para criar sistemas e redes segmentados, consolidados e seguros.

3.2.3 **Check Point SDP Control *Layer***

Check Point SDP *Control Layer* baseia-se na Check Point *Software Blade Architecture* que fornece aos clientes soluções de segurança flexíveis e eficazes para atender às suas necessidades exatas. Com a escolha de mais de 20 *Software Blades*, a natureza modular do *Software Blade Architecture* permite aos clientes

construir uma solução de segurança relevante por ponto de execução e expandir sua infraestrutura de segurança ao longo do tempo.

3.2.4 ***Next Generation Threat Prevention* Check Point**

Oferece eficientemente controles para combater muitas das ameaças conhecidas e desconhecidas. A solução de prevenção contra ameaças de ponto de acesso inclui: *Intrusion Prevention System* (IPS) para prevenir de forma proativa intrusões, antivírus de rede para identificar e bloquear *malware* , Anti-bot para detectar e prevenir dano de bot, *Threat Emulation Threat Emulation malware* sandboxing para detectar e bloquear o desconhecido e ataques zero-*day*. A Check Point criou um gigantesco gerador de dados e proteção de ameaças baseado na nuvem, o Check Point ThreatCloud ™. Check Point ThreatCloud permite uma maneira colaborativa de combater o cibercrime, oferecendo inteligência de ameaças de segurança em tempo real convertida em indicadores de segurança para a camada de controle.

3.2.5 ***Next Generation Firewall And Secure Web Gateway***

O controle de acesso Check Point baseia-se em várias *blades* de *software* que permitem uma política de segurança unificada baseada em contexto: *Firewall* para controlar com segurança o acesso a clientes, servidores, aplicativos e tipos de conexão. *Application Control* para controlar o uso de aplicativos *Web* 2.0 e evitar o uso de aplicativos de alto risco. Filtragem de URLs para controlar o acesso a milhões de *Sites* da *Web* e impedir o acesso a *Sites* que hospedam *malware* e Conhecimento de Identidade para visibilidade granular de usuários, grupos e máquinas e criação de políticas precisas e baseadas em identidade.

3.2.6 **Next Generation Data Protection**

As soluções abrangem todas as facetas de proteger o conteúdo de ficar nas mãos erradas. *Data Loss Preventio* (DLP) é parte integrante de uma solução de proteção de dados que ajuda as empresas a proteger antecipadamente informações sensíveis contra perda não intencional, educando os usuários sobre políticas adequadas de tratamento de dados e capacitando-os para remediar incidentes em tempo real. DLP controla informações sensíveis de sair da empresa e também inspeciona e controla e-mails sensíveis entre departamentos com apoio Microsoft Exchange. Além disso, a Check Point fornece proteção para dados em repouso e em armazenamento com tecnologias de criptografia. Essas tecnologias podem ser implementadas em todos os pontos de fiscalização protegendo documentos sensíveis e dados confidenciais de serem acessados ou transferidos para mídia removível ou por usuários não autorizados.

3.2.7 **Check Point *Capsule***

Check Point Capsule: Estendendo a Política Corporativa de Segurança para Dispositivos Móveis - permite estender a segurança da Check Point da rede corporativa e aplicá-la aos seus dispositivos móveis. Desta forma, tanto a rede como os dispositivos móveis de seus funcionários aplicam as mesmas proteções contra ameaças internas e externas. Com a Check Point Capsule você pode acessar e-mails corporativos, documentos e diretórios internos e como conjuntos de um ambiente de negócios seguro. Os dados pessoais e as aplicações são segregados dos dados empresariais, permitindo o uso seguro dos negócios como conjuntos, protegendo ao mesmo tempo as informações pessoais e as aplicações dos funcionários. Os documentos de negócios estão protegidos em qualquer lugar com a Check Point *Capsule*. A segurança é estabelecida na criação do documento, e viaja com o documento onde quer que vá, garantindo que as diretrizes corporativas de segurança sejam sempre cumpridas.

3.2.8 **Check Point SDP *Management Layer***

Todas as proteções e pontos de imposição do Check Point são gerenciados a partir do console de gerenciamento unificado de segurança. A gestão de segurança Check Point é altamente escalável, proporcionando a capacidade de gerir dezenas de milhões de objetos ao mesmo tempo que mantém tempos de resposta super-rápidos da interface do utilizador.

A Check Point *Security Management* suporta a segmentação empresarial, permitindo que os administradores definam a política de segurança para cada segmento, ao mesmo tempo que impõem a segregação de tarefas com um novo conceito chamado *Layers* e Sub *Layers*. As políticas podem ser definidas para cada segmento. Políticas de controle de acesso podem ser definidas usando camadas separadas, que podem ser atribuídas a diferentes administradores. Múltiplos administradores podem trabalhar na mesma política simultaneamente.

O Check Point *Security Management fornece* CLIs e APIs de Serviços *Web* que permitem às organizações se integrarem com outros sistemas, como gerenciamento de rede, CRM, solução de problemas, gestão de identidades e tratamento de nuvens.

3.2.9 **Check Point *Smartevent***

Check Point *SmartEvent* executa grande análise de dados e correlação de eventos de segurança em tempo real. Ele oferece a capacidade de fornecer uma visão consolidada e correlacionada de um incidente baseado em múltiplas fontes de informação. Análise de eventos de segurança é cria inteligência acionável sob a forma de indicadores de ameaça que podem ser distribuídos através do *ThreatCloud* para bloquear ameaças em tempo real.

4 CONCLUSÃO

Através deste estudo pode-se demonstrar e compreender a importância da segurança das redes corporativas em um mundo com infraestruturas e redes de TI de alta exigência, onde os perímetros não são mais bem definidos e onde as ameaças crescem mais inteligentes todos os dias, a escolha de definir a maneira correta de proteger as empresas na paisagem de ameaças em constante mudança.

Existe uma ampla proliferação de produtos de segurança de pontos, entretanto a escolha deve ser assertiva se baseando em aplicações que atendam a usabilidade da rede. As corporações de hoje precisam de uma única arquitetura que combine dispositivos de segurança de rede de alto desempenho com proteções proativas e em tempo real. Um novo paradigma é necessário para proteger proativamente as organizações.

Neste trabalho se destacou as soluções da Check Point que operam sob uma arquitetura de segurança unificada que permite a segurança de ponta a ponta com uma única linha de gateways de segurança unificados e permitem um único agente para toda a segurança que pode ser gerenciado a partir de um único console de gerenciamento unificado. Esse gerenciamento unificado permite a facilidade de implantação e o controle centralizado e suportado, e reforçado com atualizações de segurança em tempo real, no APÊNDICE C podemos visualizar todos os pontos fracos evidenciados pelo Check Point em uma única tela e de fácil compreensão.

Considerando o exemplo prático utilizado como referência de análise da segurança de rede, foi possível compreender a necessidade do fornecimento de uma solução única que abranja as mais diferentes variâncias de segurança existentes, a fim de ter uma gerencia unificada de segurança, cada dia mais alinhada as necessidades das empresas.

4.1 CONSIDERAÇÔES FINAIS

Neste trabalho a respeito do conceito de segurança de rede de computadores, os três questionamentos feitos inicialmente, agora podem ser respondidos, sendo o melhor sistema de segurança a ser implantado, a opção que mais se adeque ao perfil dos acessos da rede, assim como a implementação do sistema em todos os gateways, e por último, os benefícios do sistema através do gerenciamento unificado e a fácil interface que o sistema oferece, possibilitando uma rápida interpretação dos resultados.

As aplicações demonstradas têm como objetivo elucidar o funcionamento dos *firewalls,* e também demonstrar e fornecer uma base para trabalhos futuros, podendo ser aprofundados em diversos aplicações, no uso da ferramenta Check Point, que tem capacidade de proteger e controlar o fluxo de dados, o exemplo exposto demonstrou uma situação real, do qual não se difere muito dos problemas em que uma empresa enfrenta, atualmente com a preocupação de roubos de informações, principalmente ativo intelectual das corporações, esse mercado de *software* e *hardware* visando a segurança e controle de acesso, tende a um crescimento exponencial. Sugerimos também para trabalhos futuros: A implementação de diferentes fornecedores de sistemas *firewall*; comparativos entre ramos de atuação diferentes; levantar a tendência dos riscos e tipos de ferramentas que mais se adequam para uma determinada aplicação.

5 REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17799**: **Tecnologia da informação, Técnicas de segurança, Código de prática para a gestão da segurança da informação**. Rio de Janeiro: ABNT, 2005. 132p

_____. **ABNT ISO/IEC NBR 27002:2005.**

BRASIL. Decreto nº 3.505, de 13 de junho de 2000**. Institui a política de segurança da informação nos órgãos e entidades da Administração Pública Federal, e dá outras providências.** Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 14 jun. 2000.

CCOMPANY, **Serviço Gerenciado de Segurança** – *Firewall* . Disponível em: <http://www.ccompany.com.br/*firewall* .htm>. Acesso em: 19 agosto. 2016.

CERT.br. O Centro de Estudos, **Resposta e Tratamento de Incidentes de Segurança no Brasil**, Disponível em: <https://www.cert.br/>Acesso em: 19 agosto. 2016.

CHIAVENATO,I (2000) **Adiministracion de recursos Humanos**, 5ta. Ed. McGraw Hill, Colombia.

COMER, Douglas E.. **Redes de Computadores e Internet**. 2. ed. São Paulo: Bookman, 2001.

DANTAS, Mário. **Tecnologia de Redes de Comunicação e Computadores**. Rio de Janeiro: Axcel Books, 2002.

FREIRE, Alexandre. **Sistemas de Firewall e Defesa de Perímetros. Portal Módulo Security**, 2004. Disponível em: . Acesso em: 09 Out. 2011.

HOUAISS, Antonio e VILLAR, Mauro de Salles. **Dicionário Houaiss da língua portuguesa.** Rio de Janeiro: Editora Objetiva, 2001.

MICHAELIS. **Moderno Dicionário da Língua Portuguesa**. Disponível em: <http://michaelis.uol.com.br/moderno/portugues/index.php>. Acesso em: 10 junho. 2017.

NAKAMURA, Emilio T.; GEUS, Paulo L. de. **Segurança de Redes em Ambientes Cooperativos**. São Paulo: Novatec, 2007.

NETO, Urubatan. **Dominando Linux Firewall Iptables**. Rio de Janeiro: Ciência Moderna, 2004.

RIBEIRO, Olivério de Paiva. **Cultura organizacional: educação, ciência e tecnologia.** Disponível em: Pg. 3. Acesso em: set.2008.

RITTINGHOUSE, John W; RANSOME, F. James. **Cloud Computing: Implementation, Management and Security**. CRC PRESS, 2009.

SOARES, Luís Fernando; LEMOS, Guido; COLCHER, Sérgio. **Redes de computadores: das LANs, MANs e WANs às redes ATM**. Rio de Janeiro: Campus, 1995.

SPONH, Marco Aurélio**. Desenvolvimento e análise de desempenho de um "Packet Session Filter.** Porto Alegre – RS: CPGCC/UFRGS, 1997. Tese de Mestrado.

TANENBAUM, Andrew. S. **Redes de Computadores.** 4ª ed. Rio de Janeiro: Editora Campus (Elsevier), 2011.

ZWICKY, Elizabeth D.; COOPER, SIMON e CHAPMAN, D. Brent. ***Building internet firewalls***. Local: ISBN: 1-56592-871-7, Ed. O'Reilly, 2000.

APÊNDICES

APÊNDICE A - Lista com 20 *Software* que Mais Sofreram Tentativas de Transpor a Segurança Explorando Vulnerabilidades.

(continua)

Attack / Exploit	Source	Destination	Industry Reference	Events
CIFS (SMB) File Name Patterns	192.9.25.99	sonserina2.frimesa.local (192.9.24.70)	CA-2001-26	2.3K
		Total: 1 Destination	1 Reference	2.3K
	192.9.25.85	sonserina2.frimesa.local (192.9.24.70)	CA-2001-26	2.0K
		Total: 1 Destination	1 Reference	2.0K
	192.9.68.14	sonserina2.frimesa.local (192.9.24.70)	CA-2001-26	401
		Total: 1 Destination	1 Reference	401
	172.19.176.2	sonserina2.frimesa.local (192.9.24.70)	CA-2001-26	331
		Total: 1 Destination	1 Reference	331
	192.9.25.77	sonserina2.frimesa.local (192.9.24.70)	CA-2001-26	273
		Total: 1 Destination	1 Reference	273
	Total: 40 Sources	2 Destinations	1 Reference	6.8K
Microsoft Windows LNK File Shell Command Trojan	192.9.25.249	sonserina2.frimesa.local (192.9.24.70)	None	86
		Total: 1 Destination	1 Reference	86
	192.9.25.77	sonserina2.frimesa.local (192.9.24.70)	None	50
		Total: 1 Destination	1 Reference	50
	Total: 2 Sources	1 Destination	1 Reference	136
Internet Explorer iepeers.dll Remote Code Execution	172.19.182.2	172.31.106.3	CVE-2010-0806	3
		40.112.142.148	CVE-2010-0806	3
		Total: 2 Destinations	1 Reference	6
	192.9.33.16	172.31.106.3	CVE-2010-0806	1
		40.112.142.148	CVE-2010-0806	1
		Total: 2 Destinations	1 Reference	2
	172.19.186.4	172.31.106.3	CVE-2010-0806	1
		40.112.142.148	CVE-2010-0806	1
		Total: 2 Destinations	1 Reference	2
	172.19.67.1	40.112.142.4	CVE-2010-0806	1
		172.31.106.3	CVE-2010-0806	1
		Total: 2 Destinations	1 Reference	2
	192.9.212.112	40.112.142.4	CVE-2010-0806	1
		172.31.106.3	CVE-2010-0806	1
		Total: 2 Destinations	1 Reference	2
	Total: 30 Sources	3 Destinations	1 Reference	42
Microsoft Windows NT Null CIFS Sessions	172.19.71.3	192.9.1.140	CVE-2000-1200	11
		Total: 1 Destination	1 Reference	11
	172.20.80.30	192.9.1.140	CVE-2000-1200	8
		Total: 1 Destination	1 Reference	8
	192.9.67.17	192.9.1.140	CVE-2000-1200	2
		Total: 1 Destination	1 Reference	2
	172.20.112.1	192.9.1.140	CVE-2000-1200	2
		Total: 1 Destination	1 Reference	2
	172.20.20.2	192.9.1.140	CVE-2000-1200	2

(Continua)

Attack / Exploit	Source	Destination	Industry Reference	Events
Microsoft Windows NT Null CIFS Sessions	172.20.20.2	Total: 1 Destination	1 Reference	2
	Total: 5 Sources	1 Destination	1 Reference	25
Microsoft SMB Create Response Remote Code Execution (MS11-043)	172.19.72.5	192.9.200.109	CVE-2011-1268	5
		Total: 1 Destination	1 Reference	5
	192.9.45.2	192.9.200.109	CVE-2011-1268	2
		Total: 1 Destination	1 Reference	2
	172.19.176.2	192.9.200.109	CVE-2011-1268	2
		Total: 1 Destination	1 Reference	2
	172.20.96.4	192.9.200.109	CVE-2011-1268	1
		Total: 1 Destination	1 Reference	1
	172.19.70.3	192.9.200.109	CVE-2011-1268	1
		Total: 1 Destination	1 Reference	1
	Total: 10 Sources	1 Destination	1 Reference	16
Multiple Vendors OPIE Off-By-One Stack Buffer Overflow	castamere.frimesa.local (172.31.107.11)	host.labbo.com.br (50.28.30.125)	CVE-2010-1938	7
		Total: 1 Destination	1 Reference	7
	Total: 1 Source	1 Destination	1 Reference	7
Microsoft Color Control Panel Insecure Library Loading (MS12-012)	172.19.185.4	192.9.200.109	CVE-2012-5082	3
		Total: 1 Destination	1 Reference	3
	Total: 1 Source	1 Destination	1 Reference	3
Nuclear Exploit Kit Landing Page	172.31.106.3	104.24.117.148	None	1
		Total: 1 Destination	1 Reference	1
	192.9.1.77	104.24.117.148	None	1
		Total: 1 Destination	1 Reference	1
	Total: 2 Sources	1 Destination	1 Reference	2
Angler Exploit Kit Redirection	192.9.25.181	172.31.106.3	None	1
		173.236.26.18	None	1
		Total: 2 Destinations	1 Reference	2
	Total: 1 Source	2 Destinations	1 Reference	2
Microsoft Windows File and Directory Name Command Injection (MS12-048)	172.20.112.167	192.9.50.21	CVE-2012-0175	2
		Total: 1 Destination	1 Reference	2
	Total: 1 Source	1 Destination	1 Reference	2
PHP Web Shell Generic Backdoor	172.31.106.3	web2415.uni5.net (191.6.200.88)	None	1
		Total: 1 Destination	1 Reference	1
	192.9.1.208	web2415.uni5.net (191.6.200.88)	None	1
		Total: 1 Destination	1 Reference	1
	Total: 2 Sources	1 Destination	1 Reference	2
Microsoft Excel Record Structure Memory Corruption (MS12-030)	192.9.68.212	hedwig.frimesa.local (192.9.200.239)	CVE-2012-0143	2
		Total: 1 Destination	1 Reference	2
	Total: 1 Source	1 Destination	1 Reference	2
RIG Exploit Kit Landing Page	172.31.106.3	recommendation.undo.it (131.72.139.215)	None	1
		Total: 1 Destination	1 Reference	1
	192.9.50.74	recommendation.undo.it (131.72.139.215)	None	1
		Total: 1 Destination	1 Reference	1
	Total: 2 Sources	1 Destination	1 Reference	2

(conclusão)

Attack / Exploit	Source	Destination	Industry Reference	Events
Microsoft SMB Server Null Pointer Denial of Service (MS10-012)	172.19.183.4	sonserina2.frimesa.local (192.9.24.70)	CVE-2010-0022	1
		Total: 1 Destination	1 Reference	1
	Total: 1 Source	1 Destination	1 Reference	1
OpenSSL TLS Connection Record Handling Denial of Service	172.31.106.3	40.114.49.252	CVE-2010-0740	1
		Total: 1 Destination	1 Reference	1
	Total: 1 Source	1 Destination	1 Reference	1
Microsoft Windows Filename Parsing Remote Code Execution (MS12-081)	192.9.25.85	sonserina2.frimesa.local (192.9.24.70)	CVE-2012-4774	1
		Total: 1 Destination	1 Reference	1
	Total: 1 Source	1 Destination	1 Reference	1
Apple IOS and OSX WebKit Engine Denial Of Service	192.9.50.115	192.241.167.182	None	1
		Total: 1 Destination	1 Reference	1
	Total: 1 Source	1 Destination	1 Reference	1
Web Servers Suspicious File Upload	192.9.1.208	web2415.uni5.net (191.6.200.88)	None	1
		Total: 1 Destination	1 Reference	1
	Total: 1 Source	1 Destination	1 Reference	1
Total: 18 Attacks / Exploits	**94 Sources**	**15 Destinations**	**12 References**	**7.1K**

Fonte: Os Autores

APÊNDICE B - Lista com as 10 Aplicações *Web* de Alto Risco Encontradas Nesta Analise.

(continua)

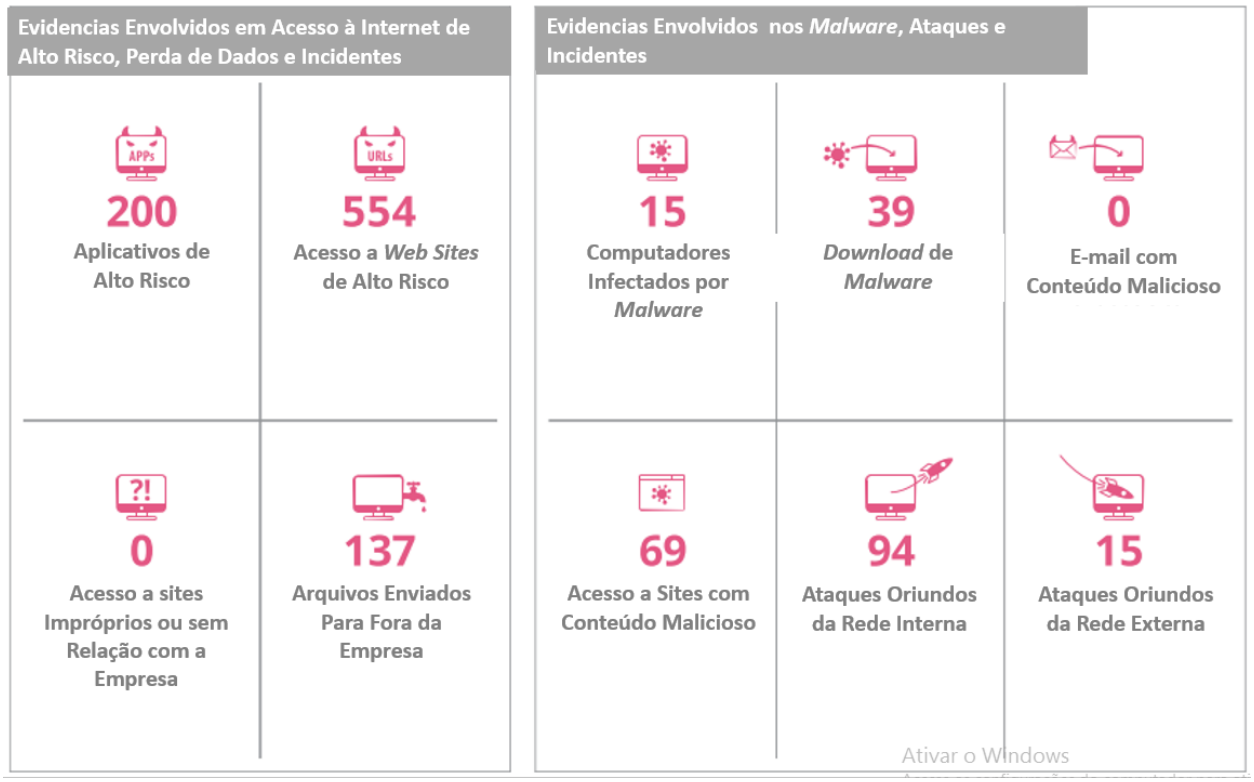
Application Category	Application Name	Source	Application Risk*	Traffic
Remote Administration	VNC	172.19.176.2 ufm-supti-c02.frimesa.local (17. ufm-supti-c13.frimesa.local (17. ufm-supti-c10.frimesa.local (17. ufm-supti-c06.frimesa.local (1... 35 more Sources	4 High	4.2GB
	Remote Desktop Protocol	172.19.64.1 172.19.64.2 172.19.65.1 172.19.65.2 172.19.65.3 90 more Sources	4 High	1.9GB
	TeamViewer	172.19.71.3 172.20.116.168 ufm-supti-c13.frimesa.local (17. ufm-supti-c01.frimesa.local (17. ufm-supti-c03.frimesa.local (17. 21 more Sources	4 High	856.3MB
	Remote Desktop Protocol 8.0	172.19.64.2 172.19.65.1 172.19.130.197 172.19.176.2 172.19.179.1 29 more Sources	4 High	112.5MB
Remote Administration	TeamViewer-web-Management Console	ufm-supti-c04.frimesa.local (172.30.2.8) 172.31.106.3 192.9.212.106	4 High	109.5MB
	Ammyy Admin	10.250.16.6 ufm-supti-c13.frimesa.local (172.30.2.2) 172.31.106.3 192.9.212.101	4 High	46.5MB
	VNC-file transfer	ufm-supti-c13.frimesa.local (172.30.2.2) 192.9.1.20	4 High	18.5MB
	AnyDesk	172.31.106.3 172.31.113.1 192.9.212.101	4 High	456.0KB
	Total: 8 Applications	**150 Sources**	**4 High**	**7.2GB**
File Storage and Sharing	Dropbox	172.19.68.2 172.19.176.1 172.19.181.1 172.19.182.4 172.19.182.7 50 more Sources	4 High	6.6GB
	Photosnack	192.9.51.27	4 High	192.0KB
	Egnyte	172.31.106.3	4 High	128.0KB
	ImageVenue	192.9.1.77 192.9.1.178 192.9.1.185 192.9.25.78 192.9.50.30 5 more Sources	4 High	112.0KB
	Clip2Net	192.9.1.141 192.9.52.83	4 High	80.0KB

(conclusão)

Application Category	Application Name	Source	Application Risk*	Traffic
File Storage and Sharing	Sugarsync	192.9.212.101	4 High	32.0KB
	Total: 6 Applications	**66 Sources**	**4 High**	**6.6GB**
P2P File Sharing	BitTorrent Protocol	192.9.1.16 192.9.55.11 192.9.212.101 192.9.212.102 192.9.212.106 2 more Sources	4 High	5.7GB
	uTorrent	192.9.52.75 192.9.212.101 192.9.212.102 192.9.212.109	4 High	15.1MB
	eMule	192.9.1.18 192.9.212.103	4 High	7.3MB
	BitTorrent Sync	192.9.212.101 192.9.212.102 192.9.212.109	4 High	296.0KB
	BitComet	192.9.212.106 192.9.212.107	4 High	24.0KB
	Total: 5 Applications	**10 Sources**	**4 High**	**5.8GB**
Download Manager	Free Download Manager	192.9.1.20	4 High	3.2GB
	Total: 1 Application	**1 Source**	**4 High**	**3.2GB**
Anonymizer	FreeGate	192.9.212.102	5 Critical	13.4MB
	SoftEther VPN	172.19.65.4	5 Critical	8.2MB
	Ultrasurf	172.31.106.3	5 Critical	3.2MB
	iodine	192.9.200.105	5 Critical	368.0KB
	Tor	192.9.36.6 192.9.212.101 192.9.212.112	5 Critical	344.0KB
	I2P	192.9.212.112	5 Critical	216.0KB
	VPN Master	192.9.212.112	5 Critical	24.0KB
	Hamachi	192.9.212.101	5 Critical	8.0KB
	VTunnel	192.9.23.16	5 Critical	8.0KB
	OpenVPN	192.9.220.1	5 Critical	8.0KB
	Total: 10 Applications	**9 Sources**	**5 Critical**	**25.8MB**
Network Protocols	Telnet Protocol	192.9.68.8	4 High	2.0MB
	X11	ufm-supti-c13.frimesa.local (172.30.2.2) ufm-supti-c13.frimesa.local (172.30.99.9)	4 High	32.0KB
	Total: 2 Applications	**3 Sources**	**4 High**	**2.0MB**
Web Content Aggregators	Docstoc	192.9.52.16 192.9.67.44	4 High	64.0KB
	Total: 1 Application	**2 Sources**	**4 High**	**64.0KB**
Computers / Internet	Norton Identity Safe	192.9.212.106	4 High	24.0KB
	Total: 1 Application	**1 Source**	**4 High**	**24.0KB**
Total: 8 Categories	**34 Applications**	**200 Sources**	**5 Critical**	**22.8GB**

Fonte: Autores

APÊNDICE C – Resultados Encontrados na Varredura Utilizando o Sistema Check Point.



Fonte: Autores