Centro Universitário de Brasília

Instituto CEUB de Pesquisa e Desenvolvimento – ICPD

DANIEL LUÍS REZENDE GUIMARÃES

UMA ANÁLISE DE RISCOS APLICADA Á TECNOLOGIA DE FIREWALLS

Brasília

2013

DANIEL LUÍS REZENDE GUIMARÃES

UMA ANÁLISE DE RISCOS APLICADA Á TECNOLOGIA DE FIREWALLS

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-Graduação Lato Sensu, na área de Rede de Computadores com ênfase em Segurança.

Orientador: Prof. José Eduardo Brandão

Brasília

2013

DANIEL LUÍS REZENDE GUIMARÃES

UMA ANÁLISE DE RISCOS APLICADA Á TECNOLOGIA DE FIREWALLS

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-Graduação Lato Sensu, na área de Rede de Computadores com ênfase em Segurança.

Orientador: Prof.José Eduardo Brandão

Brasília, 08 de julho de 2013.

Banca Examinadora

_____

Prof. Marco Antônio de O. Araújo

_____

Prof. Gilson Ciarallo

Dedicatória

Primeiramente a Deus, por sempre ter estado comigo e por ter feito com que eu crescesse adquirindo novos horizontes e aumentado os meus conhecimentos. A minha família, por sempre acreditar no meu potencial

AGRADECIMENTO

Agradeço ao professor José Eduardo Brandão, por ter me orientado e por ter me dado dicas valiosas no desenvolvimento desse trabalho, quando também me auxiliou sugerindo novos argumentos, criticando no que era preciso e sempre buscando o aperfeiçoamento. De igual modo agradeço ao professor Gilson pelas orientações de metodologia.

Agradeço aos meu colegas de turma, por terem me incentivado e pelo companheirismo prestado.

Agradeço então a todas as pessoas que contribuíram diretamente ou indiretamente para a execução e para a realização desse trabalho.

“Há sonhos que devem ser ressonhados,

projetos que não podem ser esquecidos”.

(Hilda Hilst)

RESUMO

O firewall é um importante mecanismo de segurança para proteção das redes de computadores modernos. Esse trabalho é direcionado ao estudo das vulnerabilidades encontradas nos firewall e o que fazer para mitigá-las Nesse trabalho também serão apresentados alguns conceitos básicos de segurança, bem como também dos conceitos básicos de firewall que contribuem assim na construção e utilização do mesmo. Esse trabalho tem como objetivo buscar entender algumas vulnerabilidades que são encontradas nos firewalls e o que pode se fazer para reduzir ou até mesmo evitar as falhas no uso e implementação de um firewall. Foi realizado uma pesquisa no cerco acadêmico mostrando qual é a importância dos firewalls dentro da organização, pois para isso depende de alguns fatores como: configuração e uso adequado. Sendo assim, usando os firewalls dentro das organizações, conclui-se também que apenas os firewalls não são suficientes para garantir um sistema computacional 100% seguro.Existem outros mecanismos de segurança como IDS,IPS e a VPN que, trabalhando juntamente com o firewall minimizam os ataques e garantem com isso uma performance melhor dentro da organização.

Palavras chaves: Firewall. Segurança. Vulnerabilidades

ABSTRACT

The firewall is an important security mechanism to protect the modern computer networks. This work is directed to the study of vulnerabilities found in the firewall and how to mitigate them this work will also be presented some basic security concepts, and also the basics of firewall thus contribute in the construction and use. In this work aims seek to understand some vulnerabilities that are found in firewalls and what can be done to reduce or even avoid the pitfalls in the use and implementation of a firewall. We conducted a survey in the siege academic showing what is the importance of firewalls within the organization, for to do so depends on a few factors such as configuration and proper use. Thus, using firewalls within organizations, it also follows that only the firewalls are not enough to guarantee a computing system one hundred percent safe. There are other security mechanisms such as IDS, IPS and VPN working with the firewall minimize attacks and it ensures better performance within the organization.

Keywords: Firewall. Security, Vulnerabilities

LISTA DE ABREVIATURAS E SIGLAS

CERT: The Computer Emergency Response Team

IP: Protocolo da Internet

DMZ: Zona Demilitarizada

IDS: Sistema de Detecção de Intrusos

IPS: Sistema de Prevenção de Intrusos

VPNs: Redes Privadas Virtuais

TCP: Protocolo de Controle de Transmissão

UDP: Protocolo de Datagrama de Usuário

ICMP: Protocolo de Mensagem para Controle da Internet

IGMP: Protocolo de Gestão do Grupo da Internet

POP: Protocolo de Correio

SMTP: Protocolo Simples de Transferência de e-mail

FTP: Protocolo de Transferência de Arquivo

HTTP: Protocolo de Transferência de hipertexto

LISTA DE TABELAS

LISTA DE FIGURAS

SUMÁRIO

INTRODUÇÃO

Nesse trabalho serão abordados os assuntos com relação à segurança da tecnologia de firewalls, um dos principais mecanismos de segurança das redes computacionais.

Durante o uso e implementação dos firewalls é necessário conhecer as eventuais vulnerabilidades e falhas existentes na estrutura da rede e nos próprios firewalls, bem como o que fazer para se evitar incidentes que prejudiquem o desempenho dos sistemas computacionais.

Através desse trabalho é possível também elencar os principais riscos, suas devidas consequências e por fim, as medidas preventivas para que haja um melhor funcionamento deste tipo de mecanismo na organização, de modo a garantir uma segurança na estrutura da rede.

O presente trabalho foi estruturado em 4 capítulos. Na introdução apresenta-se uma visão geral dos objetivos a serem alcançados e também de como fazer para se ter êxito nos problemas e desafios elencados na presente obra. O primeiro capítulo descreve em poucas palavras, os principais conceitos da Segurança da Informação. No segundo capítulo, há a descrição dos principais conceitos do objeto de estudo, ou seja, os firewalls. No terceiro capítulo, têm-se uma análise mais detalhado da análise de riscos dos firewalls. No quarto capítulo é apresentado um resumo da análise de riscos para aplicação em projetos de gestão de riscos.

Objetivos:

Objetivo Geral:

Estudar os riscos encontrados na escolha dos mecanismos de segurança, a saber: o firewall.

Objetivos Específicos:

Entre os objetivos específicos pode-se destacar:

- Listar os principais conceitos de segurança da informação, relacionados ao estudo dos firewalls;
- Descrever os conceitos básicos de firewall, bem como da estrutura e do funcionamento que fazem do mesmo, um dos dispositivos indispensáveis na segurança computacional; e
- Fazer o estudo dos riscos e vulnerabilidades da tecnologia de firewalls, assim como apontar as possíveis soluções para minimizar o impacto causado na sua exploração.

Justificativa:

Relevância

Segundo o CERT - Centro de Estudos, resposta, e tratamento de incidentes (2003), um *firewall* bem configurado é um instrumento importante para implantar a política de segurança da rede. Ele pode reduzir a informação disponível externamente sobre

a rede, ou, em alguns casos, até mesmo barrar ataques a vulnerabilidades ainda não divulgadas publicamente (e para as quais correções não estão disponíveis).

O CERT relata também que, por outro lado, *firewalls* não são infalíveis. A simples instalação de um *firewall* não garante que a rede esteja segura contra invasores. Um *firewall* não pode ser a sua única linha de defesa; ele é mais um dentre os diversos mecanismos e procedimentos que aumentam a segurança de uma rede.

Ainda de acordo o CERT, outra limitação dos *firewalls* é que eles protegem apenas contra ataques externos ao *firewall*, nada podendo fazer contra ataques que partem de dentro da rede por ele protegida.

Contexto

Segundo Nunes e Martins (2007), que descreve a história do Firewall, demonstra que os firewalls estão entre os desenvolvimentos mais recentes da tecnologia INTERNET. Desde o final da década de 80, o conceito de firewall começou a ser utilizado, quando roteadores separavam pequenas redes. Assim, separadas, as redes poderiam instalar aplicativos e gerenciar seus recursos da forma lhes fosse conveniente. Caso essas aplicações apresentassem algum problema, provocando o congestionamento da rede, as redes dos demais segmentos não seriam afetadas.

Os primeiros firewalls que trabalhavam a segurança de redes surgiram no início dos anos 90. Eram mecanismos que lidavam com um pequeno conjunto de regras, como: Alguém da rede A pode acessar a rede B, ou alguém da rede C não pode acessar a rede B. Esses firewalls eram efetivos, mas bastante limitados.

Apesar do esforço do Firewall em proteger a rede, não existe uma segurança totalmente confiável, pois sempre vão haver vulnerabilidades. Por outro lado

também, há o cuidado e alguns riscos que devem ser levados em conta para evitar que os computadores da organização entrem em estado de emergência.

Os problemas de segurança atuais são resolvidos de forma mais eficaz usando-se Firewalls e túneis privados virtuais. Utilitários de proteção de periféricos, como detectores de intrusão e monitores de segurança, fazem sua parte para alarmar e alertar, mas serão os FIREWALLS que continuarão sendo a base da segurança da Internet.

Pressupostos

Esse trabalho tem como fundamento, analisar os riscos e vulnerabilidades encontradas nos firewalls, presente na literatura. Tais referências podem não esgotar todas as possibilidades, mas trazem informações suficientes para o início de uma análise mais aprofundada no futuro.

Esse documento não traz instruções de exploração das vulnerabilidades apresentadas, limitando-se à organização das informações teóricas sobre o assunto.

Formação do problema

Ao longo dessa pesquisa serão respondidas as seguintes perguntas:

- Como funciona o firewall?
- Quando os riscos foram apresentados, quais serão as consequências e as contra-medidas para se evitar o pior?
- Quais as boas práticas no uso e implementação do firewall?

Premissas

Este trabalho leva em consideração as seguintes hipóteses:

- Os firewalls não são mecanismos de segurança perfeitos e podem conter vulnerabilidades;
- É possível encontrar na literatura informações suficientes para montagem de uma análise das vulnerabilidades dos firewalls; e
- É possível determinar contramedidas teóricas para mitigar as vulnerabilidades dos firewalls.

PROCEDIMENTOS METODOLÓGICOS

Basicamente, com a finalidade de atingir o objetivo principal deste estudo, foi realizada uma pesquisa na literatura relacionada a firewall, mostrando os aspectos mais relevantes no que se refere à questão de se usar o firewall como segurança de uma empresa. Entre os aspectos relevantes com relação à segurança, esse trabalho tem como fundamento ser um guia inicial para as pessoas que necessitam conhecer e se aprofundar mais nesse tema de segurança. A partir dessa pesquisa serão descritos alguns riscos e vulnerabilidades encontrados em firewalls, bem como as medidas que poderão controlar esses riscos, permitindo com isso uma maior segurança.

As informações coletadas foram organizadas de maneira a auxiliar a tomada de decisão dos profissionais de segurança da informação, com o objetivo de mitigar possíveis riscos às suas organizações.

1 SEGURANÇA DA INFORMAÇÃO

Segundo Sêmola (2003), a Segurança da Informação é uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade.

De acordo com o mesmo autor, a Segurança da Informação pode ser definida como a prática de gestão de riscos de incidentes que impliquem no comprometimento dos três principais conceitos de segurança: confidencialidade, integridade e disponibilidade da informação.

A seguir serão apresentados alguns conceitos relacionados aos assuntos abordados nesse documento.

1.1 Princípios básicos da Segurança da Informação

A Segurança da Informação tem como objetivo a preservação de três princípios básicos pelos quais se norteiam a implementação desta prática. Segundo Sêmola (2003), podemos definir:

a) Confidencialidade: Toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando a limitação de seu acesso e uso apenas às pessoas para quem elas são destinadas.

b) Integridade: Toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-las contra alterações indevidas, intencionais ou acidentais.

c) Disponibilidade: Toda informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível aos seus usuários no momento em que os mesmos delas necessitem para qualquer finalidade.

1.2 Outros conceitos

a) Informação: Conjunto de dados utilizados para a transferência de uma mensagem entre indivíduos e/ou máquinas em processos comunicativos (baseados em troca de mensagens) ou transacionais (processos em que sejam realizadas operações que envolvam, por exemplo, a transferência de valores monetários).

A informação pode estar presente ou ser manipulada por inúmeros elementos deste processo, chamados ativos, os quais são alvo de proteção da segurança da informação (SÊMOLA, 2003).

b) Ativo: Um ativo é todo elemento que compõe os processos que manipulam e processam a informação, a contar a própria informação, o meio em que ela é armazenada, os equipamentos em que ela é manuseada, transportada e descartada.

O termo ativo possui esta denominação, oriunda da área financeira, por ser considerado um elemento de valor para um indivíduo ou organização, e que, por esse motivo, necessita de proteção adequada (ISO/IEC-17799).

Existem muitas formas de dividir e agrupar os ativos para facilitar seu tratamento, como por exemplo: equipamentos, aplicações, usuários, ambientes, informações e processos. Desta forma, torna-se possível identificar melhor as fronteiras de cada

grupo, tratando-os com especificidade e aumentando qualitativamente as atividades de segurança (SÊMOLA,2003)

1.3 Aspectos associados à Segurança da Informação

Alguns elementos são considerados essenciais na prática da segurança da informação, dependendo do objetivo que se pretende alcançar.

a) Autenticação: processo de identificação e reconhecimento formal da identidade dos elementos que entram em comunicação ou fazem parte de uma transação eletrônica que permite o acesso à informação e seus ativos por meio de controles de identificação desses elementos (SÊMOLA,2003)

b) Autorização: concessão de uma permissão para o acesso às informações e funcionalidades das aplicações aos participantes de um processo de troca de informações (usuário ou máquina), após a correta identificação e autenticação dos mesmos (SÊMOLA,2003).

c) Auditoria: processo de coleta de evidências de uso dos recursos existentes, a fim de identificar as entidades envolvidas num processo de troca de informações, ou seja, a origem, destino e meios de tráfego de uma informação (SÊMOLA,2003).

d) Autenticidade: garantia de que as entidades (informação, máquinas, usuários) identificadas em um processo de comunicação como remetentes ou autores sejam exatamente o que dizem ser e que a mensagem ou informação não

foi alterada após o seu envio ou validação. Normalmente, o termo autenticidade é utilizado no contexto da certificação digital (SÊMOLA, 2003).

e) Irretratabilidade: característica de informações que possuem uma identificação do seu emissor que o autentica como o autor de informações por ele enviadas e recebidas. Sinônimo de não-repúdio (SÊMOLA, 2003).

1.4 Ameaças

Agentes ou condições que causam incidentes que comprometem as informações e seus ativos por meio da exploração de vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade e, consequentemente, causando impactos aos negócios de uma organização (SÊMOLA, 2003).

Classificando as ameaças quanto a sua intencionalidade, elas podem ser divididas nos seguintes grupos (SÊMOLA, 2003).

a) Naturais: ameaças decorrentes de fenômenos da natureza, como incêndios naturais, enchentes, terremotos, tempestades, eletromagnéticas, maremotos, aquecimento, poluição etc.

b) Involuntárias: Ameaças inconscientes, quase sempre causadas pelo desconhecimento. Podem ser causadas por incidentes, erros, falta de energia etc.

c) Voluntárias: Ameaças propositais causadas por agentes humanos como atacantes, invasores, espiões, ladrões, criadores e disseminadores de vírus de computador, incendiários.

1.5 Vulnerabilidades

Fragilidade presente ou associada a ativos que manipulam e/ ou processam informações que, ao ser explorada por ameaças, permite a ocorrência de um incidente de segurança, afetando negativamente um ou mais princípios da segurança da informação: confidencialidade, integridade e disponibilidade.

As vulnerabilidades por si só não provocam incidentes, pois são elementos passivos, necessitando para tanto de um agente causador ou condição favorável, que são as ameaças (SÊMOLA, 2003).

Exemplos de vulnerabilidades:

a) Físicas: Instalações prediais fora do padrão; salas de CPD mal planejadas; falta de extintores, detectores de fumaça e de outros recursos para combate a incêndio em sala com armários e fichários estratégicos, risco de explosões, vazamentos ou incêndio.

b) Naturais: Computadores são suscetíveis a desastres naturais, como incêndios, enchentes, terremotos, tempestades, e outros, como falta de energia, acúmulo de poeira, aumento de umidade e de temperatura etc.

c) Hardware: Falhas nos recursos tecnológicos (desgaste, obsolescência, má utilização) ou erros durante a instalação.

d) Software: Erros na instalação ou na configuração podem acarretar acessos indevidos, vazamento de informações, perda de dados ou indisponibilidade do recurso quando necessário.

e) Mídias: Discos, fitas, relatórios e impressos podem ser perdidos ou danificados. A radiação eletromagnética pode afetar diversos tipos de mídias magnéticas.

f) Comunicação: Acessos não autorizados ou perda de comunicação.

g) Humanas: Falta de treinamento, compartilhamento de informações confidenciais, não execução de rotinas de segurança, erros ou omissões; ameaça de bomba, sabotagens, distúrbios civis, greves, vandalismo, roubo, destruição da propriedade ou dados, invasões ou guerras.

1.6 Riscos

Probabilidade de ameaças explorarem vulnerabilidades, provocando perdas de confidencialidades, integridade e disponibilidade, causando, possivelmente, impactos nos negócios (SÊMOLA, 2003).

1.7 Impacto

Abrangência dos danos causados por um incidente de segurança sobre um ou mais processos de negócio (SÊMOLA, 2003).

1.8 Incidente

Fato (evento) decorrente da ação de uma ameaça, que explora uma ou mais vulnerabilidades, levando à perda de princípios da segurança da informação: confidencialidade, integridade e disponibilidade.

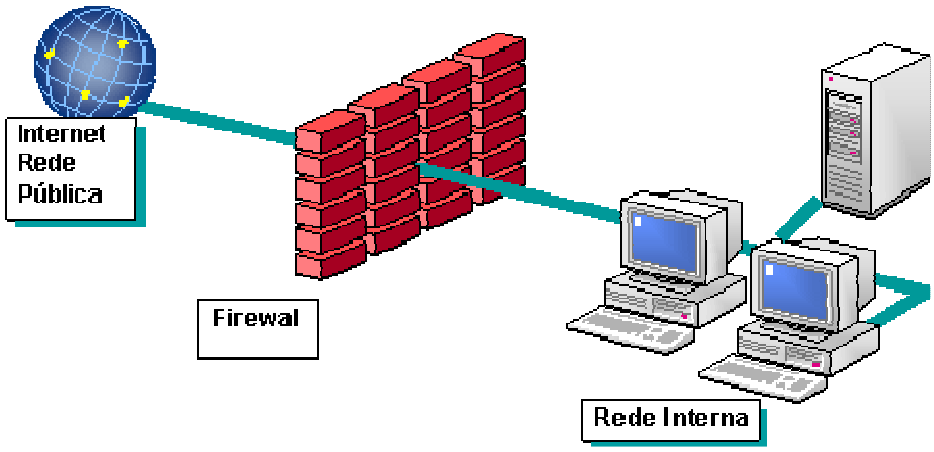
Um incidente gera impactos aos processos de negócios da empresa, sendo ele o elemento a ser evitado em uma cadeia de gestão de processos e pessoas.

A gravidade de um incidente pode ser analisada em termos qualitativos e quantitativos, sendo medida pelo seu impacto. (SÊMOLA, 2003).

2 CONCEITOS DE FIREWALL

Conforme o autor Cheswick (2005), um firewall é qualquer dispositivo, software, arranjo ou equipamento utilizado que limita o acesso à rede. A figura 1 demonstra uma simples implementação de firewall.

Figura 1- Exemplo de arquitetura de rede com firewall



Fonte: Disponível em: http://www.juliobattisti.com.br/tutoriais/breinerqueiroz/isaserver2k001.asp. Acesso em: 18 ago. 2012.

Na utilização dos firewalls é possível criar regras, impedindo assim que informações indesejadas trafeguem na rede. Na atualidade, os firewalls podem vir dentro de muitos dispositivos como: roteadores, modems, dentre outros equipamentos. Dessa forma, os firewalls são indispensáveis quando se trata de segurança de rede. É de se notar também, que outros mecanismos de segurança trabalham juntamente com os firewalls, como: Filtro de Pacotes, Firewall de Aplicação, Proxy, DMZ (*Demilitarized Zone*), IDS (*Intrusion Detection System*), IPS (*Intrusion Prevention System*) e VPNs (*Virtual Private Networks*- Redes privadas virtuais). Embora se tenha o uso desses dispositivos na rede, não há nada 100% seguro, mas usando-se

adequadamente esses mecanismos, diminuem assim os riscos e falhas existentes na rede.

Como existem diversas visões quanto aos seus tipos, para essa pesquisa serão classificados a seguir.

2.1 Funcionamento do Firewall

Há três principais categorias principais de funcionamento de um firewall: filtro de pacotes, firewall de aplicação e Proxy. Em seguida, será descrito qual é a importância e a relevância dessas categorias no estudo de firewall.

2.1.1 Filtragem de pacotes

Filtro de pacotes é o processo de seletivamente permitir ou bloquear o tráfego de pacotes entre duas redes, fazendo uso de um conjunto de regras de filtragem. Estas regras são baseadas em informações existentes nos cabeçalhos de cada pacote e, logo, a filtragem é feita em cada pacote de uma sessão individualmente (CHAPMAN,1992).

Segundo Cheswick e Bellovin (2005), os filtros de pacotes podem fornecer um nível barato e útil de segurança de rede. Os filtros funcionam eliminando pacotes com base em seus endereços de origem ou destino, ou nos números de porta. Pouco ou nenhum contexto é mantido; as decisões são tomadas unicamente com base no conteúdo do pacote atual. Dependendo do tipo de dispositivo que a implementa, a filtragem pode ser feita na interface de entrada, na interface de saída, ou em ambas.

Conforme os autores Strebe e Perkins (2002) há dois tipos básicos de filtragem de pacotes:

- Padrão ou filtragem de pacotes sem estados (*stateless*)
- Filtros de pacotes com inspeção de estados (*statefull*).

2.1.1.1 Filtragem de pacotes sem estados (*stateless*)

Os filtros podem ser configurados para operar com base em qualquer parte do cabeçalho do protocolo, mas a maioria só pode ser configurada para filtrar os campos de dados mais úteis, como: o Tipo de protocolo, Endereço IP, Porta TCP/ UDP, número de fragmento e Informações sobre o roteamento de origem.

a) **Filtragem de protocolos**: essa filtragem filtra os pacotes com base no conteúdo do campo do tipo de protocolo IP. Então, o campo de protocolo pode ser utilizado para discriminar todo um conjunto de serviços, como: UDP, TCP,ICMP e IGMP.

b) **Filtragem de endereços IP**: permite limitar as conexões para e de hosts e rede específicos com base em seus endereços IP. Um ponto bem importante é que um filtro só pode limitar os endereços com base no conteúdo do campo que identifica o endereço IP.

c) **Portas TCP/UDP**: são aquelas habitualmente mais utilizadas na filtragem porque seu campo de dados indica mais especificamente para que serve o pacote. Diferentemente do que acontece na filtragem de IPs, o bloqueio de algumas portas ainda é útil, pois a maior parte das atividades dos atacantes se concentra somente em alguns protocolos específicos. Sendo assim, os protocolos mais importantes que devem ser bloqueados são: Telnet, POP, dentre outros.

d) **Roteamento de Origem**: é o processo de definir a rota exata que um pacote deve tomar entre hosts em uma conexão IP. O roteamento de origem é usado com

frequência pelos atacantes porque com ele é possível colocar qualquer endereço no campo de origem e ainda assim garantir que o pacote será retornado especificando o endereço de sua própria máquina na rota de origem.

e) **Fragmentação:** a fragmentação foi desenvolvida para suportar a passagem de pacotes IP grandes por roteadores que não podem encaminhá-los devido a restrições de tamanho de quadro existentes entre interfaces de tecnologias distintas.

Os filtros de pacotes sem estados (*stateless*) sofrem de dois problemas que impedem que sejam totalmente eficazes:

- Eles não verificam a parte útil de dados dos pacotes.
- Eles não guardam o estado das conexões.

Esses problemas fazem com que os filtros sem estado sejam insuficientes se aplicados sozinhos para proteger uma rede.

2.1.1.2 Filtros de pacotes com inspeção de estados (*statefull*)

Segundo Strebe e Perkins (2002), os filtros de pacotes *stateless* têm várias falhas, todas nascendo do fato de que um único pacote em uma comunicação não contém informações suficientes para determinar se ele deve ou não ser recusado, porque ele faz parte de uma comunicação maior. Porém, os filtros de pacotes de inspeção com estados (*statefull*) resolvem esse problema retendo na memória os estados de todas as comunicações passando pelo firewall e usando esse estado guardado para determinar se os pacotes individuais devem ou não ser abandonados. A inspeção com estados filtra fluxos de comunicação inteiros, não apenas os pacotes.

Ainda segundo Strebe e Perkins (2002), os filtros de pacotes com estados lembram-se do estado das conexões da rede e das camadas da sessão gravando informações sobre o estabelecimento da sessão que passa através do gateway do filtro. Os filtros usam então essa informação para discriminar pacotes de retorno válido, das tentativas de conexão inválidas ou de invasão. Por outro lado, também, os filtros de pacotes com estados não permitem nenhum serviço passar pelo firewall, a não ser que esteja programado para isso

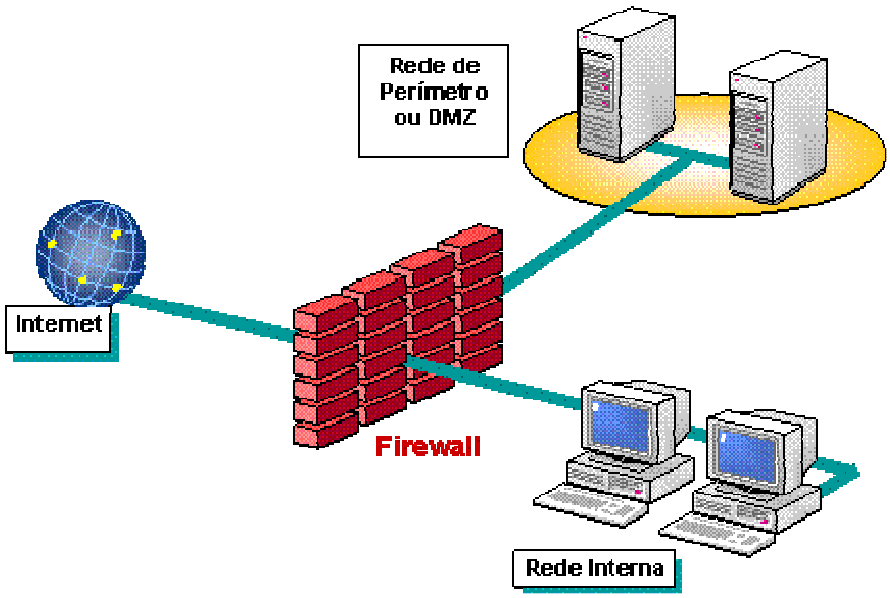
2.2 Mecanismos de segurança associados

2.2.1 Demilitarized Zone (DMZ)

A DMZ é uma pequena rede inserida em uma “zona neutra” entre a rede corporativa da empresa e a rede pública externa conforme ilustrado na figura 2. A DMZ previne o acesso direto de usuários externos aos servidores da empresa. (BAUMRUCKER et al., 2006).

Segundo Queiroz (2005), a DMZ ou rede de perímetro seria a exposição de determinada área da rede interna para publicar determinados serviços à internet. Configuramos uma DMZ com o auxílio de firewall para que somente as portas e/ou protocolos que interessam sejam desbloqueados e assim diminuindo ao máximo a exposição para a internet. A DMZ é tipicamente usada para disponibilizar para usuários da internet servidores de e-mail e servidores Web.

Figura 2- Exemplo de DMZ



Fonte:Disponível em: http://www.juliobattisti.com.br/tutoriais/breinerqueiroz/isaserver2k001.asp. Acesso em 19. ago.2012

2.2.2 Sistemas de Detecção de Intrusão (IDS)

Sistemas de Detecção de Intrusão (IDS) são dispositivos que analisam o tráfego da rede, procurando indicação de uma invasão.(CHESWICK et al., 1994).

2.2.3 Sistema de Prevensão à Intrusão (IPS)

Ao contrário de sistemas IDS que atuam de forma passiva na rede, sistemas IPS possuem mecanismos (baseados em software ou hardware) que o permitem agir de forma pró-ativa (SIQUEIRA,2003), possibilitando dessa forma que ataques, conhecidos ou não, sejam identificados com antecedência e medidas de prevenção, para inibir o sucesso, sejam tomadas de forma automática (DESAI,2003).

2.2.4 VPN

Segundo Barbosa (2012), Redes Privadas Virtuais, também denominadas de VPN, permitem a conexão com segurança de duas redes separadas fisicamente sem que espiões possam observar o conteúdo dos pacotes que trafegam entre estas redes.

Consoante Barbosa (2012), uma VPN pode estar sujeita a tentativas de redirecionamento ou outros tipos de interceptações enquanto o túnel estiver sendo estabelecido, mas, quando implementadas como parte integrante de um *firewall*, os serviços de autenticação e segurança do *firewall* podem ser utilizados para evitar a exploração enquanto o túnel estiver sendo estabelecido.

2.2.5 Firewall de aplicação

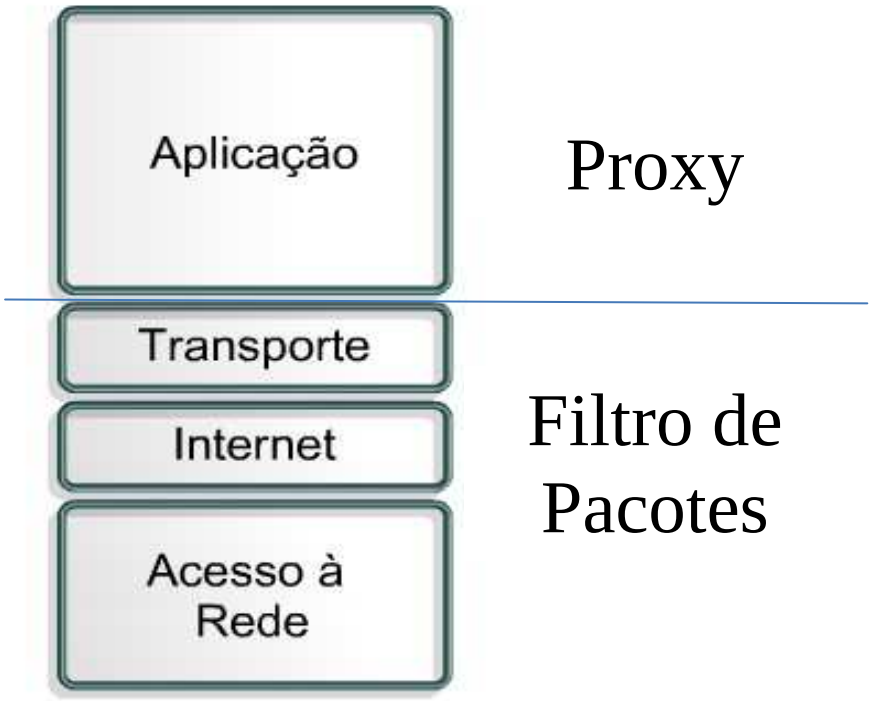
O papel de um firewall de aplicação é melhorar a segurança de uma determinada aplicação através de conhecimentos específicos sobre ela (BYRNE, 2009). Segundo Alecrim (2004), Firewalls de controle de aplicação (exemplos de aplicação: SMTP, FTP, HTTP, etc) são instalados geralmente em computadores servidores e são conhecidos como *proxy*. O *Proxy* é uma parte importante da arquitetura web, pois oferecem uma otimização que pode diminuir a latência e reduzir a carga sobre os servidores (COMER, 2006). Servidores Proxy podem ser, por exemplo, aplicações especializadas em um firewall que assumem as requisições dos usuários de uma rede para o serviço HTTP.

É de se notar que a principal diferença entre Proxy e filtro de pacotes é que o Proxy atua na camada de aplicação, enquanto o filtro de pacotes atua nas camadas de

rede e transporte. Outro ponto interessante e relevante para os nossos estudos, é que os firewalls baseados em Proxy sempre foram mais lentos que aqueles baseados em filtragem de pacotes com informações de estado.

Modelo TCP/IP

Figura 3- Pilha TCP/IP



Fonte: Disponível em < http://gridra.wordpress.com/category/uncategorized/> Acesso em: 3 set.2012

Na Figura 3, a camada de Aplicação é destinada ao Proxy e a camada de Transporte e a Internet são destinadas ao Filtro de Pacotes.

O *proxy* não permite comunicação direta entre a rede e a Internet. Tudo deve passar por ele, que atua como um intermediador. O proxy efetua a comunicação entre ambos os lados por meio da avaliação do número da sessão TCP dos pacotes. Este

tipo de firewall é mais complexo, porém muito seguro, pois todas as aplicações precisam de um proxy. Caso não haja, a aplicação simplesmente não funciona. Em casos assim, uma solução é criar um "proxy genérico", através de uma configuração que informa que determinadas aplicações usarão certas portas.

O firewall de aplicação permite um acompanhamento mais preciso do tráfego entre a rede e a Internet (ou entre a rede e outra rede). É possível, inclusive, contar com recursos de registro de eventos (logs) e ferramentas de auditoria.

3 VULNERABILIDADES EM FIREWALLS

Os firewalls não são os únicos mecanismos de segurança em uma organização. Assim, como no capítulo anterior desse trabalho foi falado do IPS e IDS que juntamente com o firewall fornecem uma maior segurança para o ambiente virtual. Mas também não há sistema 100% seguro, pois sempre vão existir falhas e vulnerabilidades novas, fazendo com que haja uma preocupação com o sistema a ser utilizado. Nesse capítulo serão analisadas as principais vulnerabilidades encontradas em firewalls.

Segundo Kamara et al. (2003), a vulnerabilidade do firewall é definida como um erro cometido durante o desempenho do firewall, implementação, configuração ou, que pode ser explorada para atacar a rede de confiança que o firewall é designado a proteger. Ainda segundo essa autor, nas vulnerabilidades descritas por ele, os firewalls podem ser testados e mapeados para se evitar esses erros, podendo causar maiores problemas na rede.

Ainda segundo esse autor, as causas mais comuns de vulnerabilidades encontradas em firewalls são: Erros de Validação, Erros de Autorização, Serialização, Erro de Verificação do Limite e Erro de Domínio.

Segundo Geus e Pouw (1996), algumas vulnerabilidades na arquitetura do firewall são encontradas como: falhas no software; vulnerabilidade do meio físico; negação de serviços e ataques de baixo nível que possam afetar a disponibilidade, a confidencialidade e a integridade das informações.

A seguir essas vulnerabilidades serão descritas e apresentadas as ações para mitiga-las. As vulnerabilidades a seguir foram baseadas nos trabalhos de Kamara et al. (2003) e de Pouw e Geus (1996).

3.1 Erro de validação:

Causa: Segundo Kamara et al. (2003), ocorre quando o programa interage com o ambiente sem garantir a correção de dados ambientais. Existem três tipos de dados ambientais que necessitam de validação. Validação de entrada que garante que a entrada é o esperado. Validação de origem que assegura a identidade do IP de origem e a Validação de destino que assegura que a informação vai para o lugar que é suposto, ou seja, isto inclui a garantia que as informações protegidas não vão para um alvo não confiável. No erro de validação ocorre consequências no protocolo TCP/IP, que segundo Geus e Pouw (1996), a principal deficiência do protocolo TCP/IP é a incapacidade de autenticar uma máquina na rede, em outras palavras, com base no endereço IP de origem de um pacote recebido, é impossível determinar com certeza a identidade da máquina que o tenha originado, impossibilitando com isso a validação das informações corretas que trafegam na rede.

Consequências: Consoante Barbosa (2012), os ataques que exploram tal falha têm como tática mais comum a personificação de uma máquina na rede. A finalidade é a de obter informações sigilosas como senhas, abusar da confiança que as máquinas mantêm entre si, até ações mais sutis e sofisticadas como alterar o conteúdo dos dados que estejam de passagem para outros destinos, afetando com isso a Disponibilidade, Integridade e a Confidencialidade das informações.

Medidas preventivas: Segundo Geus e Pouw (1996), podemos ter algumas medidas preventivas como:

- Isolar a Rede privada: o objetivo principal de um firewall, é restringir o acesso direto de máquinas externas à rede privada. A ideia é reduzir os alvos potenciais de N para 1, no caso o firewall.

- Desativar roteamento dinâmico: é necessário estabelecer roteamento estático.

3.2 Erro de autorização:

Causa: Segundo Kamara et al. (2003), um erro de autorização, chamado de erro de autenticação na origem, permite uma operação protegida a ser invocado sem verificação suficiente da autoridade do agente de chamada. Conforme Geus e Pouw (1996), as senhas ainda continuam sendo usadas como principal forma de autenticação da internet. A facilidade de se forjar este tipo de sistema é notória e vem sendo explorada desde os tempos primórdios da rede.

Consequências: Ocorrendo esse erro, pode ocorrer que os firewalls fiquem inseguros e vulneráveis a ataques, permitindo com isso que dados sigilosos sejam acessados. Segundo Von Zuben e Henriques (2009), pode-se ter vazamento de informações, permitindo assim, furto de dados e informações, afetando com isso a disponibilidade e a confidencialidade das informações. Conforme Von Zuben e Henriques (2009) também, pode-se ter: comprometimento de senhas: por meio de senhas compartilhadas, fracas, afetando assim a Disponibilidade e Confidencialidade das informações.

Medidas Preventivas: Conforme Von Zuben e Henriques (2009), existem algumas medidas eficazes que se enquadram nesse caso. Por isso pode-se ter: auditoria de logs: o registro de eventos de segurança, exceções e atividades de usuários permite o rastreamento de problemas e a identificação da autoria de uma ação; Política de senhas, ou seja, implementação de políticas que definam regras para formação, proteção e uso de senhas amenizando com isso acesso não autorizado aos sistemas computacionais e Política de acessos, ou seja, implementação de políticas de privilégio mínimo

3.3 Serialização:

Causa: Segundo Kamara et al. (2003), um erro de serialização permite que o comportamento assíncrono de operações de sistemas diferentes a ser explorado pode causar uma violação de segurança.

Consequências: Através do Erro de Serialização, segundo Kamara et al. (2003), pode-se ter que uma falha ocorra quando por exemplo, quando tem-se dois nomes ou número de IPs para uma mesma máquina, fazendo com que haja ambiguidade nos sistema computacionais, ocorrendo erro na estrutura, afetando os dados ou até informações importantes, isso de forma inesperada e repentina, prejudicando a Integridade e a Confidencialidade das Informações.

Medidas preventivas: No Erro de Serialização, têm-se como visto anteriormente, um problema de rede. Para poder corrigir esse erro é necessário crias alguns mecanismos de identificação desse tipo de erro ou então fazer uma mitigação para amenizar ou diminuir com esses tipos de erro. Contudo para isso, faz-se importante

ter um firewall bem configurado, Segundo Von Zuben e Henriques (2009), firewalls e redes locais fisicamente inseguras devem mapear endereços físicos de maneira estática, isso faz com que a rede evite permitir duplicação de endereços.

3.4 Erro de verificação de limite:

Causa: Segundo kamara et al. (2003), é causada por falhas em verificar os limites e garantir restrições. Não verificar valores associados com o tamanho da tabela, de alocação de arquivos, ou consumo de outros recursos, leva a erros de verificação de limite. O *Buffer overflor* (Sobrecarga de memória intermediária) é um resultado de um erro de verificação de limite.

Consequências: Conforme Von Zuben e Henriques (2009), se por exemplo os dados forem maior do que o permitido vai haver uma extrapolação maior que o permitido, com certeza ocorrerá erro. Nesse erro pode ocorrer erros de softwares, ou seja, a exploração de falhas de codificação como *buffer-overflow* e falta de verificação de argumentos permite elevação de privilégios e acesso não autorizado, prejudicando assim a Disponibilidade, a Integridade e a Confidencialidade das informações.

Medidas preventivas: Conforme Von Zuben e Henriques (2009), algumas medidas preventivas podem fazer com que sejam minimizados esses riscos, tai como: instalação de correções de segurança: permite eliminar vulnerabilidades conhecidas e já corrigidas pelos fabricantes de softwares amenizando assim a sobrecarga da memória intermediária. Outras medidas preventivas são: Controle de Fluxo e

Controle de Congestionamento. Segundo o LARC- Laboratory of Computer Networks and Architecture (2002), da Universidade de São Paulo (USP), no Controle de Fluxo, tem-se uma ação preventiva, através de notificações e policiamento, impedindo assim que exceda o limite permitido. Já quando se fala no Controle de Congestionamento, tem-se a ação corretiva, ou seja, caso exceda o limite, corrige os erros causados por esse tipo de erro.

3.5 Erro de domínio:

Causa: Segundo Kamara et al. (2003), um erro de domínio ocorre quando os limites pretendidos entre ambientes de proteção tem “buracos”. Isso faz com que as informações da rede sejam afetadas e vaze, sendo acessadas por pessoas mal intencionadas.

Consequências: Segundo Kamara et al. (2003), algumas consequências são apontadas que se enquadram nesse erro:

- Execução de código: Isso ocorre quando uma vulnerabilidade pode levar a código que está sendo executado de forma ilegítima. Isto inclui, mas não está limitado a, o código escrito por um intruso. Uma má configuração do código pode levar a erros no Domínio do Servidor podendo afetar a Disponibilidade, Integridade e a Confidencialidade.

- Mudança de recurso de destino: Isso ocorre quando uma vulnerabilidade permite que o estado de um recurso a ser ilegitimamente alteradas por um atacante. Um recurso pode ser um host, uma tabela de regras de firewall, ou qualquerentidade que deve ser protegido pelo firewall, afetando com isso a Disponibilidade, a Integridade e a Confidencialidade das informações.

Medidas preventivas: De acordo com Von Zuben e Henqiues (2009), as medidas que ajudarão no controle desse erro são: desativação de serviços desnecessários: a redução do número de serviços executados na máquina reduz a possibilidade de existência de vulnerabilidades não resolvidas; Auditoria de logs: o registro de eventos de segurança, exceções e atividades de usuários permite o rastreamento de problemas, a identificação da autoria de uma ação e Instalação automática de atualizações: permite que novas versões do software cliente sejam automaticamente atualizadas, ajudando assim a segurança do sistema. Daí surge a necessidade de se ter um firewall bem configurado, de modo a não permitir que esses erros de domínio possam ocorrer sem deixar com isso “buracos” ou “vazios” em sua estrutura

3.6 Falhas de software

Causa: Conforme Geus e Pouw (1996), são comportamento inesperado de programas, quer seja por falha de projeto e/ou implementação. Quanto maior a complexidade e tamanho de um programa, mais difícil é “ prever” seu comportamento e consequentemente garantir que este apresente falhas que possam comprometer a segurança do sistema a qual pertença.

Consequências: Conforme Von Zuben e Henriques (2009), algumas falhas são de se esperar, com relação aos erros apresentados nos softwares, dentre elas se destacam: instalações indevidas: instalação não autorizada do software cliente, afetando com isso a Disponibilidade, a Integridade e a Confidencialidade das informações.

Medidas preventivas: Por essa razão, ao instalar um firewall, algumas medidas devem ser consideradas tendo em vista amenizar falhas de software na segurança dos firewalls. Segue algumas medidas segundo Geus e Pouw (1996):

- Manter a configuração “minimal”: quer dizer que deve-se executar o mínimo número de processos necessários para garantir a funcionalidade desejada, e preferencialmente processos mais simples e pequenos, que possam assim ser testados durante o processo de implementação;

- Restringir ao máximo os privilégios dos processos: essa restrição é importante, pois garante assim apenas os privilégios necessários no sistema, para que os mesmo possam assim desempenhar suas funções.

- Manter software atualizado de correções e falhas: os programas em execução em um firewall devem corresponder à última versão no que se refere a correção de falhas de segurança.

3.7 Vulnerabilidades do meio físico

Causas: Conforme Geus e Pouw (1996), As deficiências da tecnologia ethernet, que constitui a maior parte das redes locais, expõem ainda mais as fragilidades da

Internet. Os principais problemas estão relacionados com: a facilidade de se realizar grampo e o falso mapeamento entre endereço de rede (IP) e endereço fixo (ARP).

Consequências:

Conforme Geus e Pouw (1996), podemos ter 2 consequências:

- Grampeando a Rede: Sendo ethernet uma tecnologia de rede onde o meio físico é compartilhado, é possível configurar a interface de rede de uma máquina em modo “promíscuo”, e assim receber todos os quadros transmitidos no meio. Geralmente tem-se por objetivo obter informações privilegiadas, como por exemplo senhas, mas também pode usar tal facilidade como passo na implementação de ataques mais sofisticados, afetando assim a Confidencialidade das informações.

- Falso Mapeamento entre Endereço IP e Endereço Ethernet (ARP): o protocolo ARP (Address Resolution Protocol) mapeia um endereço IP em endereço ethernet enviando um broadcast com o endereço IP desejado. A máquina que tiver o endereço IP procurado, ou alguma outra agindo em nome daquela, responde com o par: endereço IP- endereço ethernet. Uma máquina mal intencionada pode então enviar respostas falsas, desviando todo o tráfego para si, tendo como objetivo personificar uma máquina, ou mais sutilmente, modificar os dados que estiverem sendo transmitidos entre duas outras máquinas, afetando com isso a Integridade das informações.

Medidas preventivas. Conforme Von Zuben e Henriques (2009), pode-se ter:

- Política de senhas: implementação de políticas que definam regras para formação, proteção e uso de senhas;
- Política de acessos: implementação de políticas de privilégio mínimo;
- Firewalls e redes locais fisicamente inseguras devem mapear endereços físicos de maneira estática

3.8 Negação de serviços (Denial of Service Attacks):

Causa: Segundo Kamara et al. (2003), Isso ocorre quando uma vulnerabilidade é explorada para interromper um serviço prestado ao usuário legítimo. Serviços no contexto pode variar de encaminhamento de pacotes ou tradução de endereços de rede da administração.

Consequência: Conforme Geus e Pouw (1996), durante a negação de serviços há a interrupção de funcionamento de serviços de um computador ou sistema, por meio da saturação de seus recursos, afetando com isso a Disponibilidade e a Integridade das informações.

Medidas preventivas: Conforme Geus e Pouw (1996), a geração de “logs” e análise periódica de dados armazenados, é ainda a melhor forma de se lidar com este tipo de problema; restringir acesso a usuários comuns, ajuda também a minimizar acesso não autorizado a intenções indesejáveis de usuários que tentam burlar o sistema e outra medida importante no combate a esse tipo de erro é procedimentos de Tuning, pois além de uma prática recomendada em geral, têm

efeito significativo na disponibilidade do sistema, que na verdade é também considerado um fator de medida de segurança.

3.9 Ataques de baixo nível:

Causa: Consoante Geus e Pouw (1996), os firewalls estão sujeitos a ataques de baixo nível que exploram deficiências nas implementações das camadas mais baixas do protocolo TCP/IP, e também por sondagens externas que procuram por tais vulnerabilidades.

Consequências: Através desse ataque pode-se afetar a Disponibilidade e a Integridade das informações.

Medidas Preventivas: Segundo Geus e Pouw (1996), Internet Scanners, como são chamadas as ferramentas de soldagem de rede, têm por objetivo procurar por serviços e falhas que possam comprometer um firewall e eliminar ou minimizar esse tipo de erro. A maior parte destas ferramentas baseia-se no estabelecimento de uma conexão TCP com todas as portas de uma máquina, de maneira a determinar se estas estão ativas ou não. Há também segundo esse mesmo autor, um programa chamado Scanner Detectors, que possuem a capacidade de contabilizar todas as conexões efetuadas, e a partir daí determinar a ação de tais scanners, podendo evitar com isso o Ataque de Baixo Nível das camadas inferiores do protocolo TCP/IP.

4 PROPOSTA DE CORRELACIONAMENTO DE VULNERABILIDADES

Abaixo, há algumas tabelas, relacionadas aos riscos, as consequências, as contramedidas e por fim uma tabela correlacionando todos esses elementos citados. Isso vai garantir um maior entendimento do assunto.

No quadro 1, serão descritos os riscos enumerados no trabalho, bem como o que cada risco representa facilitando com isso o entendimento das vulnerabilidades encontradas em um firewall.

Quadro 1 – Vulnerabilidades causadas no uso e implementação de um firewall

VULNERABILIDADES (V)	DESCRIÇÃO
V1- Erro de validação	Ocorre quando o programa interage com o ambiente sem garantir a correção de dados ambientais.
V2- Erro de autorização	Permite uma operação protegida a ser invocado sem verificação suficiente da autoridade do agente de chamada.
V3- Serialização	Um erro de serialização permite que o comportamento assíncrono de operações de sistemas diferentes a ser explorado pode causar uma violação de segurança.
V4- Erro de verificação de limite	Causada por falhas em verificar os limites e garantir restrições.
V5- Erro de domínio	Um erro de domínio ocorre quando as fronteiras entre ambientes de proteção destinados tem “buracos”. Isso faz com que a informação implicitamente vaza.
V6- Falhas de software	São comportamento inesperado de programas, quer seja por falha de projeto e/ou implementação.
V7- Vulnerabilidades do meio físico	As deficiências da tecnologia ethernet, que constitui a maior parte das redes locais, expõem ainda mais as fragilidades da Internet
V8- Negação de serviços	Isso ocorre quando uma vulnerabilidade é explorada para interromper um serviço prestado ao usuário legítimo.
V9- Ataques de baixo nível	Os firewalls estão sujeitos a ataques de baixo nível que exploram deficiências nas implementações das camadas mais baixas do protocolo TCP/IP

Fonte: Elaborado pelo autor do trabalho

Nesse quadro, serão enumeradas as consequências que se pode obter, devido aos riscos apresentados, bem como o conceito das mesmas, facilitando com isso a compreensão.

Quadro 2 Consequências causadas no uso e implementação de um firewall

CONSEQUÊNCIAS (C)	DESCRIÇÃO
C1- DISPONIBILIDADE	Garante que uma informação estará disponível para acesso no momento desejado.
C2- INTEGRIDADE	Garante que o conteúdo da mensagem não foi alterado ou violado indevidamente.
C3- CONFIDENCIALIDADE	Garantir que a informação só será acessível por pessoas autorizadas.

Fonte: Elaborado pelo autor do trabalho

O quadro a seguir, enumera as medidas preventivas devido aos riscos apresentados anteriormente. Essa listagem facilitará os estudos relacionados as vulnerabilidades encontradas nos firewalls.

Quadro 3 Medidas preventivas no uso e implementação de um firewall

MEDIDAS PREVENTIVAS (M)	DESCRIÇÃO
M1	Isolar a Rede Privada
M2	Desativar Roteamento Dinâmico
M3	Auditoria de Logs
M4	Políticas de Senhas
M5	Políticas de Acesso
M6	Instalação de Correções de Segurança
M7	Controle de Fluxo
M8	Controle de Congestionamento
M9	Desativação de Serviços desnecessários
M10	Identificação da Autoria de uma ação
M11	Instalação Automática de Atualizações
M12	Manter a Configuração “Minimal”
M13	Restringir ao máximo os privilégios dos processos
M14	Manter software atualizado de correções e falhas
M15	Mapeamento de endereços físicos de maneira estática
M16	Geração de logs
M17	Análise Periódica de dados armazenados

M18	Restringir acesso a usuários comuns
M19	Procedimentos de Tuning
M20	Internet Scanners

Fonte:Elaborado pelo autor do trabalho

Nesse quadro, há um correlacionamento dos riscos, gerando consequências e o que fazer para mitigar esses riscos. Pode-se ter mais de uma consequência para cada risco e mais de uma medida preventiva também.

Quadro 4 Quais as consequências e devidas medidas preventivas nos riscos apresentados.

Vulnerabilidades	Consequências	Medidas Preventivas
V1	C1, C2 e C3	M1 e M2
V2	C1 e C3	M3,M4,M5 e M11
V3	C2 e C3	M15
V4	C1,C2 e C3	M6, M7 e M8
V5	C1,C2 e C3	M3,M9,M10 e M11
V6	C1,C2 e C3	M12,M13 e M14
V7	C2 e C3	M4,M5 e M15
V8	C1 e C2	M16,M17,M18 e M19
V9	C1 e C2	M20

Fonte: Elaborado pelo autor do trabalho

Para exemplificar a utilização dos quadros, se pode ter: Erro de Validação (V1), vai ter como consequências afetando diretamente C1 (Disponibilidade), C2 (Integridade) e C3 (Confidencialidade), mas pode evitar essa vulnerabilidade através de algumas medidas preventivas: M1 (Isolar a Rede Privada) e M2 (Desativar Roteamento Dinâmico); Erro de Autorização (V2), vai ter como consequências afetando diretamente C1 (Disponibilidade) e C3 (Confidencialidade), mas pode evitar essa vulnerabilidade através de algumas medidas preventivas: M3 (Auditoria de Logs), M4 (Políticas de Senhas) ,M5 (Políticas de Acesso) e M10 (Identificação da Autoria de uma Ação); Erro de Serialização (V3), vai ter como consequências afetando diretamente C2 (Integridade) e C3 (Confidencialidade), mas pode evitar essa vulnerabilidade através de algumas medidas preventivas: M15 (Mapeamento de Endereços Físicos de Maneira Estática); Erro de Verificação do Limite (V4), vai ter como consequências afetando diretamente C1 (Disponibilidade), C2 (Integridade) e C3 (Confidencialidade), mas pode evitar essa vulnerabilidade através de algumas medidas preventivas: M6 (Instalação de Correções de Segurança), M7 (Controle de Fluxo) e M8 (Controle de Congestionamento); Erro de Domínio (V5), vai ter como consequências afetando diretamente C1 (Disponibilidade), C2 (Integridade) e C3 (Confidencialidade), mas pode evitar essa vulnerabilidade através de algumas medidas preventivas:M3 (Auditoria de Logs), M9 (Desativação de Serviços Desnecessários), M10 (Identificação da Autoria de uma Ação) e M11 (Instalação Automática de Atualizações).

CONCLUSÃO

O firewall é de fato um dos principais mecanismos de segurança da rede de uma organização, porém, os seus responsáveis não podem achar que estão completamente seguros apenas por ter um firewall atualizado e bem configurado, outras ferramentas e técnicas de segurança como: IDS, IPS devem ser implantadas a fim de dificultar a ação dos invasores.

Durante a execução desse trabalho, notou-se a importância das boas práticas na implementação e uso de um firewall, ajudando com isso a minimizar os ataques contra a estrutura computacional utilizando-se mecanismos de segurança como o firewall, foco desse trabalho.

Por isso a implementação de um firewall é recomendado:”modelo de teste”.

Na execução desse trabalho, foi demonstrado como funciona o firewall, bem como as principais partes que o integram. Durante esse trabalho foram apresentados alguns riscos que contribuem para que os analistas das rede se preocupem ainda mais com a segurança das empresas e companhias, buscando assim alternativas, de modo a eliminar ou minimizar impactos causados por essas vulnerabilidades. Os riscos poderão levar à algumas consequências, mas por sua vez terão soluções para reduzir ou eliminar os riscos existentes. E, por fim, algumas melhores práticas foram descritas, com o objetivo de se ter um conhecimento mínimo de se evitar, quando se utilizam os firewalls como mecanismos de segurança, é claro que tudo depende também da configuração e do modo como os firewalls se dispõem na rede. Através desse trabalho, espera-se uma maior compreensão dos riscos que pode haver durante o uso e implementação de um firewall.

Trabalhos futuros:

E com isso espera-se também que, com a contribuição desse trabalho, algumas hipóteses sejam sugeridas como testes que envolvam não somente a teoria, mas principalmente a prática, fazendo com que haja um maior entendimento do que se deseja propor para os trabalhos futuros. Nas próximas pesquisas faz-se importante estudar mais a fundo o firewall do sistema operacional Linux, a saber: iptables. Pois através do iptables é possível a criação de tabelas de regras, que possibilitarão uma maior segurança da rede contra invasores que procuram achar alguma falha ou brecha na rede, entre outras facilidades que permitem estabelecer um sistema mais forte e poderoso contra eventuais erros. Como trabalhos futuros pode-se propor a implantação de um firewall com os serviços de VPN e IDS trabalhando em conjunto, ambos irão proporcionar um aumento considerável no perímetro de segurança de rede da empresa, podendo esses e outros mecanismos de segurança trabalharem mais juntos afim de proporcionarem uma integração do sistema de redes segura.

REFERÊNCIAS

ALECRIM, Emerson. O que é firewall? **conceitos e tipos.** Disponível em <http://www.infowester.com/firewall.php> Acesso em: 17 jul.2012.

BAUMRUCKER, Tate; CAESAR, James; KRISHNAMURTHY, Mohan; SHINDER, Thomas W, PINKARD, Becky; SEAGREN, Eric; HUNTER, Laura. Designing and building enterprise DMZs. Syngress.Rockland.2006

BARBOSA , Ákio Nogueira .UM SISTEMA PARA ANÁLISE ATIVA DE COMPORTAMENTO DE *FIREWALL.Disponível em* <http://www.lsi.usp.br/~volnys/academic/trabalhos-orientados/Um-sistema-para-analise-ativa-de-comportamento-de-firewall.pdf>. Acesso em:27 set.2012.

BYRNE, Paul; Application firewalls in a defence-in-depth design.2009.

CERT-Práticas de Segurança para Administradores de Redes Internet. Disponível em < http://www.cert.br/docs/seg-adm-redes/>Acesso em:20 jun.2012.

CHAPMAN, D. Brent. Network (In) Security through IP packet filtering. In proceedings of the Third USENIX Unix Security Symposium, 1992.

CHESWICK, William R; BELLOVIN, Steven M; Rubin, Aviel D.Firewalls e segurança na Internet; repelindo o hacker ardiloso,2ª.ed.São Paulo:Bookman, 2005.

COMER, E. Douglas;Interligação em Rede com TCP/IP.São Paulo: Campus, 2006.

DESAI, Neil; Intrusion Prevention Systems: The Next Step in the Evolution of IDS. Disponível em : <http://www.securityfocus.com/infocus/1670>.Acesso em: 20 ago.2012.

QUEIROZ, Breiner Araujo. CONHECENDO O ISA SERVER 2000. Disponível em <http://www.juliobattisti.com.br/tutoriais/breinerqueiroz/isaserver2k001.asp> Acesso em: 18 ago.2012.

GEUS, Paulo Lício de; POUW, Keesje Duarte.Uma análise das vulnerabilidades dos firewalls.Disponível em <http://www.las.ic.unicamp.br/paulo/papers/1996-WAIS-keesje.pouw-vulnerabilidades.firewalls.pdf> Acesso em:06 out.2012.

NUNES,Pedro Henrique; MARTINS, Leonardo Dias.HISTÓRIA do Firewall, A.2007. Disponível em: <http://www.gta.ufrj.br/grad/07_1/firewall/index_files/Page350.htm> Acesso em:22 jun.2012

KAMARA, Seny et al. Analysis of vulnerabilities in internet firewalls.**Computers & Security**, v. 22, n. 3, p. 214-232, 2003.

LARC- Laboratory of Computer Networks and Architecture. Capítulo 5- Evolução das Redes. Disponível em < www.lsi.usp.br/~cranieri/pcs2476p1c5.pdf> Acesso em: 29 abril.2013.

ROBERTO Alexandre.Introdução à camada de Transporte.2008.Disponível em: < http://gridra.wordpress.com/category/uncategorized/> Acesso em:3 set.2012.

SÊMOLA, Marcos. **Gestão da Segurança da Informação, Uma visão Executiva.**Rio de Janeiro:Elsevier,2003.

SIQUEIRA, D; Intrusion Prevention Systems- Security Silver Bullet. Disponível em:<http://www.highbeam.com/doc/1G1-98710095.html>.Acesso em: 20 ago.2012.

STREBE, Matthew; PERKINS,Charles. **Firewalls**: uma fonte indispensável de recursos para os administradores de sistemas.São Paulo:Makron Books, 2002.

VON ZUBEN, M.; HENRIQUES, M. A.A. Análise de vulnerabilidades e incidentes de segurança em grades de computação voluntária. Disponível em: <http://www.lbd.dcc.ufmg.br/colecoes/sbseg/2009/016.pdf>. Acesso em: 29 set. 2012