UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
TELEINFORMÁTICA E REDES DE COMPUTADORES

RODRIGO DE ARRUDA SCHEER

SEGURANÇA EM PEQUENAS EMPRESAS

MONOGRAFIA

CURITIBA
2012

RODRIGO DE ARRUDA SCHEER

SEGURANÇA EM PEQUENAS EMPRESAS

Monografia apresentada como requisito parcial à obtenção do título de Especialista em Teleinformática e Redes de Computadores, da Universidade Tecnológica Federal do Paraná.

Orientador: Prof. Msc. Lincoln Herbert Teixeira

CURITIBA

2012

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Diretoria de Pesquisa e Pós-Graduação do *Campus* Curitiba
Departamento Acadêmico de Eletrônica
Especialização em Teleinformática e Redes de Computadores

TERMO DE APROVAÇÃO

Segurança para Pequenas Empresas

por

Rodrigo de Arruda Scheer

Esta monografia foi apresentada às 16h00min do dia 06 de Junho de 2012 como requisito parcial para a obtenção do título de ESPECIALISTA EM TELEINFORMÁTICA E REDES DE COMPUTADORES, Universidade Tecnológica Federal do Paraná. O candidato foi argüido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado com a nota 7,0 (SETE INTEIROS).

Prof. Msc. Lincoln Herbert Teixeira
(UTFPR)

Prof. Dr. Walter Godoy Júnior
(UTFPR)

Visto da Coordenação

Prof. Dr. Walter Godoy Júnior
Coordenador do Curso

RESUMO

SCHEER, Rodrigo de Arruda. **Segurança em pequenas empresas.** 2012. Monografia – Programa de Pós-Graduação em Teleinformática e Redes de Computadores, Universidade Tecnológica Federal do Paraná. Curitiba, 2012.

Atualmente tudo ao redor é ou existe uma maneira de se efetuar o processo por meio eletrônico, mas com toda a comodidade e facilidade deste tipo de acesso por outro lado existem diversos problemas com relação à segurança das informações que transitam por este meio, por isto devem-se ter ferramentas que ajudem a tornar este meio mais seguro para utilização, neste sentido empresas em geral precisam tomar ainda mais cuidados nestes quesitos, pois estes, podem se tornar facilmente alvo de ataques maliciosos, visando deixar as redes de pequenas empresas mais seguras proponho esta solução que se torna muito viável para implantação neste tipo de mercado utilizando as ferramentas de virtualização, proxy e firewall todos em um mesmo equipamento.

Palavras-chave: Proxy (Squiq). Firewall (IPTABLES). Virtualização.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

Com a utilização de computadores e principalmente da internet nos dias atuais é comum às empresas se depararem com diversos problemas que devem ser tratados e não apenas ignorados; o principal deles é com a segurança no acesso aos dados disponibilizados pela empresa, pois praticamente tudo que é feito atualmente depende de algum meio eletrônico.

As informações devem ser preservadas em qualquer tipo de empresa, todas sem exceção devem se preocupar com ela, pois um envio de e-mail para um concorrente, por exemplo, pode ocasionar prejuízos incalculáveis para uma organização.

Deve-se iniciar o processo de segurança desde o treinamento dos usuários sobre as boas práticas de informática e bem como ferramentas e serviços dentro da rede para tornar esta cada vez mais segura e confiável.

O objetivo deste projeto é o desenvolvimento de uma ferramenta que visa à proteção de redes para pequenas empresas utilizando ferramentas de baixo custo e com capacidade de proteção excelente.

O crescimento do mundo virtual fez com que as empresas ofereçam cada vez mais meios eletrônicos para comunicação, armazenamento e softwares para gerenciamento; por isso necessita-se de mecanismos para combater possíveis falhas de segurança, como vazamento de informações ou até mesmo tentativas de roubo de informações utilizando-se de possíveis falhas no planejamento da rede de uma organização.

Para o estudo deste caso abordarei algumas ferramentas utilizadas atualmente para segurança em ambiente virtual; são elas: Firewall (IPTABLES), Proxy (SQUID), IDS (SNORT), Virtualização.

Firewall (IPTABLES): Uma das ferramentas mais utilizadas e consolidadas para software livre que é utilizado geralmente para filtrar pacotes que trafegam via meio eletrônico, deixando trafegar somente o necessário, pacotes que não tem interesse são diretamente descartados e para esconder de minha rede interna assim dificultando o acesso as informações por acesso de uma rede externa.

Proxy (SQUID): Ferramenta também das mais utilizadas e consolidadas para software livre, mas esta tem como principais características o controle de acesso a sites indesejados, e o controle da cache, este para que consultas a sites externos a organização fiquem armazenados em memória para não ser necessária a consulta ao meio externo todas as vezes que forem solicitados.

IDS (SNORT) – Ferramenta utilizada para identificação de possíveis acessos indesejados a minha rede, depois de identificado uma possível ameaça pode-se encontrar uma solução para uma possível falha, ou mesmo para poder identificar responsáveis e tomar uma medida referente à tentativa de acesso a minha rede.

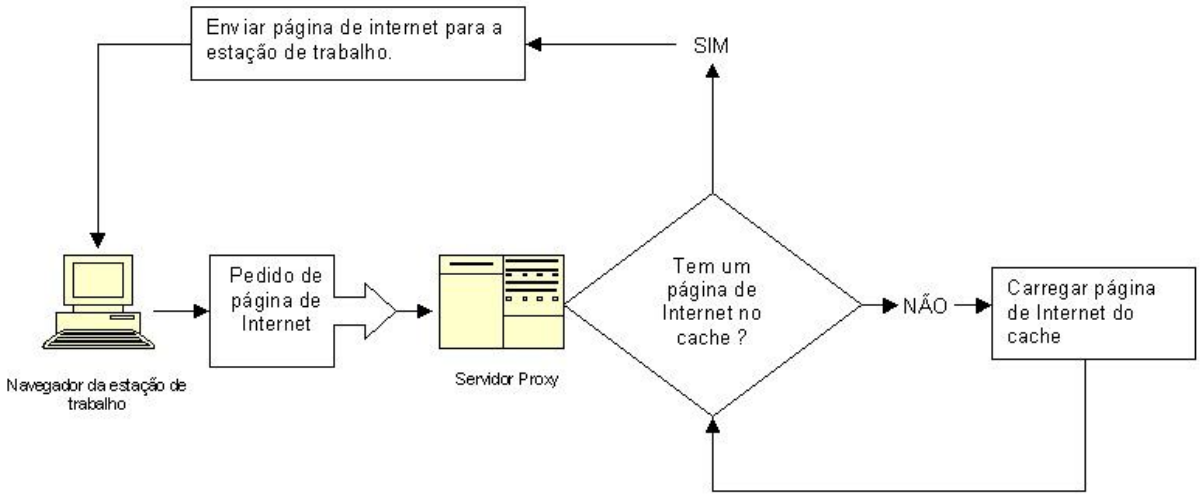
Virtualização – Consiste de um software onde é possível criar diversas instalações de sistemas operacionais diferentes dentro de uma mesma maquina física, ajudando assim a diminuir custo mobiliário e utilizar o equipamento de uma maneira mais ampla, pois muitas vezes quando tem uma maquina para cada serviço acaba por não utilizar toda a capacidade computacional da mesma.

2 PROXY (SQUID)

O Proxy Squid é uma ferramenta que não se pode abrir mão para montar um esquema de segurança para empresas, pois, se trata de um filtro de pacotes HTTP onde podemos controlar o acesso das estações, definir regras para acesso a URLs, armazenar conteúdos em cache e histórico de acessos para efetuar uma auditoria.

2.1 COMO FUNCIONAM

O Proxy aguarda uma requisição interna (Firewall, Rede interna), verifica se ele tem armazenado esta solicitação em cache, se esta, está disponível, responde para o cliente a resposta, se não, passa esta para o servidor remoto (Rede Externa), recebe a resposta armazena as informações em cache e envia para estação cliente que solicitou.



Fluxo 1: Fluxo das solicitações Servidor Proxy

Fonte: http://www.mlaureano.org/guias_tutoriais/GuiaInstSquid.htm

2.2 VANTAGENS

As principais vantagens de um Proxy Squid são o armazenamento de conteúdos em cache, otimizando muito utilização do link de internet, definir regras para acesso a URLs, controlo de acesso IP.

2.3 DESVANTAGENS

Não se pode utilizar somente um Proxy Squid e acreditar que esta seguro, esta ferramenta torna-se eficaz quando em conjunto com um Firewall, por exemplo, é montado toda uma estrutura de segurança; na questão de atualizações existe um outro ponto complicado, pois, dependendo da maneira como foi configurado o bloqueio de URLs, por exemplo, estar atualizando sempre, afinal a cada dia surgem milhares de novos sites.

3 - FIREWALL

Um Firewall tornou-se uma das ferramentas mais importantes, quando o assunto é segurança no meio eletrônico, sua principal funcionalidade desde sua concepção é a filtragem de pacotes, mas existem muitas outras funções que foram incorporadas a ferramenta devido à necessidade de se criar um meio mais seguro para utilização de serviços de rede.

Usa-se um firewall para tornar o meio eletrônico organizacional mais seguro, através dele é possível disciplinar o tráfego existente entre hosts e redes; também especificar quais os tipos de protocolos e serviços que podem ser disponibilizados interna ou externamente bem como compartilhar o acesso a internet de uma rede interna para que esta não tenha contato direto com o meio externo, ou seja, pode-se limitar o uso de serviços e ter um controle de quais redes são autorizadas a realizar determinadas funções e host confiável a executar funções especifica.

Firewall's tem um papel importante na estrutura de segurança de uma rede, sendo um dos principais itens necessários, mas não pode deixar de comentar que ele não é 100% seguro, pois possíveis falhas de protocolos ou má utilização dos usuários ele não consegue prever, um usuário que utiliza uma senha fraca (data de nascimento, aniversário de casamento, etc.) uma vez descoberta a senha ele vai liberar o acesso, pois ele está configurado a aceitar conexões provenientes deste usuário; outro erro comum é acreditar que um firewall consegue proteger as redes de "vírus" ou "worms" , por exemplo, mais uma vez o grande problema é o mau uso do usuário que acaba caindo em ciladas encaminhadas via e-mail ou mesmo através de pen-drives inseridos na máquina sem a verificação prévia de um antivírus, sendo este, o antivírus, a principal ferramenta para prevenção destes problemas.

3.1 TIPOS DE FIREWALL

3.1.1 Firewall Filtro de Pacotes

O tipo de firewall que é utilizado para controlar o fluxo dos pacotes que passam por ele e para a rede local em que ele controla, direcionando as informações para o destino correto. Para isto define-se um conjunto de regras previamente e estas direcionam a informação para o local definido.

3.1.2 Firewall NAT

É o tipo de firewall que se utiliza para esconder a rede local da internet, neste caso somente o firewall é conectado diretamente a rede externa e a rede interna somente podem sair para internet através do firewall tendo todo seu fluxo de informações registradas.

3.1.3 Firewall Híbrido

É o tipo de Firewall que engloba as duas versões anteriores, criando uma ferramenta de segurança bem mais robusta.

4 VIRTUALIAÇÃO

4.1 O QUE É?

É uma ferramenta que permite executar diversas máquinas virtuais diferentes dentro de um mesmo hardware físico, possibilitando assim uma melhor utilização dos equipamentos ainda mais levando em consideração que para um melhor gerenciamento e segurança das redes é definido uma máquina para cada serviço nessas redes, utilizando a virtualização, em uma maquina física pode-se criar diversas maquinas separadamente para efetuarem os mesmos serviços separados como de costume.

4.2 COMO FUNCIONAM

Pode-se utilizar a virtualização basicamente de duas formas, na primeira delas instalando um sistema operacional base (Windows ou Linux), neste é instalado o servidor de virtualização e dentro deste servidor são instaladas as maquinas virtuais que o usuário deseja utilizar.

Figura 1: Modelo de Virtualização dependente de um Sistema Operacional

Fonte: http://www.hardware.com.br/artigos/ferramentas-virtualizacao/

Outra maneira de se utilizar é com os chamados Hypervisors que nada mais é do que um sistema operacional que é capaz de gerenciar as os recursos computacionais e disponibilizá-los para criação de maquinas virtuais.

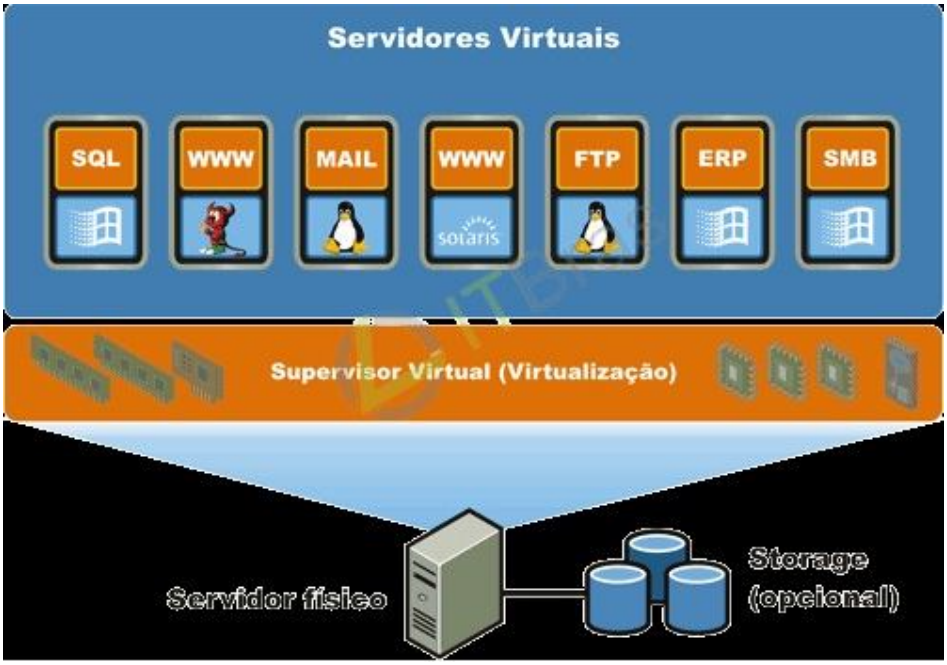


Figura 2: Modelo de Virtualização utilizando Hypervisor

Fonte: http://vembajr.wordpress.com/category/wake-up-africa/

4.3 VANTAGENS DE UM AMBIENTE VIRTUALIZADO

1. Redução de Custos – Pois utilizando este tipo de solução pode-se adquirir um número menor de equipamentos físicos para instalação dos sistemas.

2. Obter uma melhor utilização dos recursos – Pois da maneira como geralmente são configurados os serviços de rede as maquinas físicas não são utilizadas em sua total capacidade e utilizando a virtualização explora-se melhor a capacidade do equipamento.

3. Melhor gerenciamento dos servidores, com um número menor de pessoas para efetuar este controle.

4. Flexibilidade de sistema operacional – utilizam-se sistemas operacionais diferentes de uma maneira simples e rápida.

5. Uma maior facilidade de se fazer um upgrade tanto de sistema como no caso de hardware bem como o backup das maquinas.

5 DESENVOLVIMENTO/PROJETO

Antes de começar a descrever a solução proposta, sempre vale lembrar que simplesmente adotar ferramentas somente para dizer que a empresa possui soluções de segurança como Firewall, Proxys, Antivírus, entre outros; não adianta de nada se algumas mudanças na postura e na organização da empresa se não forem implantadas. Políticas de segurança e principalmente o treinamento dos usuários, explicar a importância destas medidas para o bom funcionamento das atividades diárias e com isso consequentemente a empresa em si terá um melhor controle de atividades.

5.1 POLÍTICAS DE SEGURANÇA

A primeira prática a ser adotada é o controle de acesso às estações através de usuário e senha, esta senha tem como requisito um número mínimo de caracteres (oito) e contém letras, números e caracteres especiais como (@, !, #, $), se a empresa tiver implantado um controlador de domínio (AD ou LDAP) deve-se definir que a cada 30 dias esta senha seja alterada e conforme os registros deste controlador de domínio, as últimas três senhas utilizadas não podem ser definidas como novas senhas. Nos casos onde controladores de domínio não são adotados, tem que ser definido as estações para que necessite ser criados usuários e senha para acesso às mesmas, e é claro que explicar a importância de se efetuar a troca de senha após um período de tempo que esta já utilizada. Outro item importante é deixar sempre estes usuários criados, tanto quando for criado via controlador de domínio como quando criado diretamente na estação, deve-se deixar estes usuários sempre que possível como usuários restritos não permitindo assim a instalação de alguns programas e de alterações em registros importantes do sistema operacional.

A segunda prática que se deve utilizar é o acesso à informação, ou seja, definir corretamente qual usuário tem acesso a quais tipos de informação, separar estas informações por setor e classificação de sigilo; por exemplo, um usuário que trabalha no setor de almoxarifado não pode ter acesso às informações e documentos que um usuário que trabalha no setor financeiro, também se deve deixar uma área em comum para acesso de todos.

Outra prática, a terceira, será efetuar os registros de todos os acessos à internet e dos arquivos efetuado pelos usuários, principalmente para o caso de efetuar alguma operação ilegal, como acesso a locais proibidos ou algum outro tipo de operação via internet, é possível encontra-lo, no caso dos arquivos tem de ter os registros de qualquer tipo de movimentação que é efetuada como arquivo.

Agora a principal prática a ser adotada, a quarta, é também a mais complicada, consiste no treinamento e conscientização do usuário; é necessário conscientizar o usuário que sua senha é pessoal, da importância de se utilizar senhas “difíceis”, de não deixar sua estação livre como seu usuário configurado, que o e-mail que utiliza com o endereço @NOMEDAEMPRESA.COM é o seu sobrenome deve respeitar e utilizar o mesmo com consciência e somente para fins profissionais, do cuidado ao navegar na internet, principalmente com relação aos e-mails não desejados; dos prejuízos que ele mesmo pode ter de não ter tomar estes cuidados ao utilizar pen-drives, pois este pode conter vírus, pode comprometer toda a rede, não somente sua estação e também com as informações que nele contém em muitos casos estes pen-drives possui muitas informações valiosas da empresa, tendo que tomar ainda mais cuidado para os mesmos não for perdidos.

Agora que foi definido algumas práticas que vão ajudar a ter uma rede ainda mais segura, passa-se para a solução proposta por este projeto, que consiste na utilização de uma máquina física e através da virtualização são criadas duas maquinas virtuais, uma irá utilizar como Firewall e a outra como Proxy (Squid) e IDS (Snort); para este projeto (laboratório) foi utilizado o software Virtual Box, para gerenciamento das máquinas virtuais; Debian 6.0 como sistema operacional básico das maquina virtuais e configuração dos servidores propostos; todas estas ferramentas instaladas em estação padrão utilizando o Windows Sete.

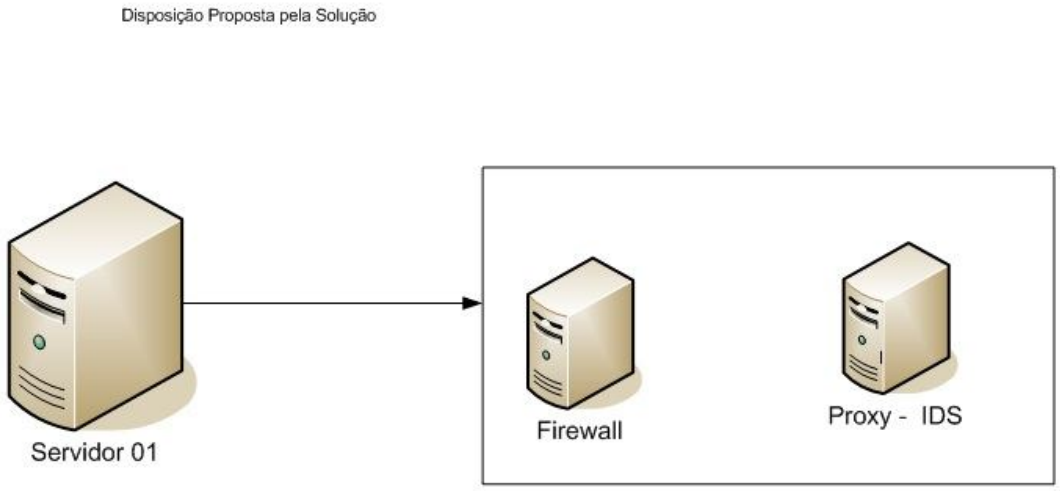


Figura 3: Modelo Proposto pela solução

Fonte: Autoria Própria

No caso de uma implantação em uma empresa propriamente dita, a melhor solução encontrada seria a utilização dos chamados Hypervisor's este sim implantam uma pequena camada de sistema operacional nas estações definidas para tal fim preparando todos os recursos físicos disponíveis para utilização das máquinas virtuais que serão criadas para disponibilização de serviços.

5.2 ESTRUTURA DE REDE

A estrutura de rede que deverá disponibilizar deve ser a seguinte:

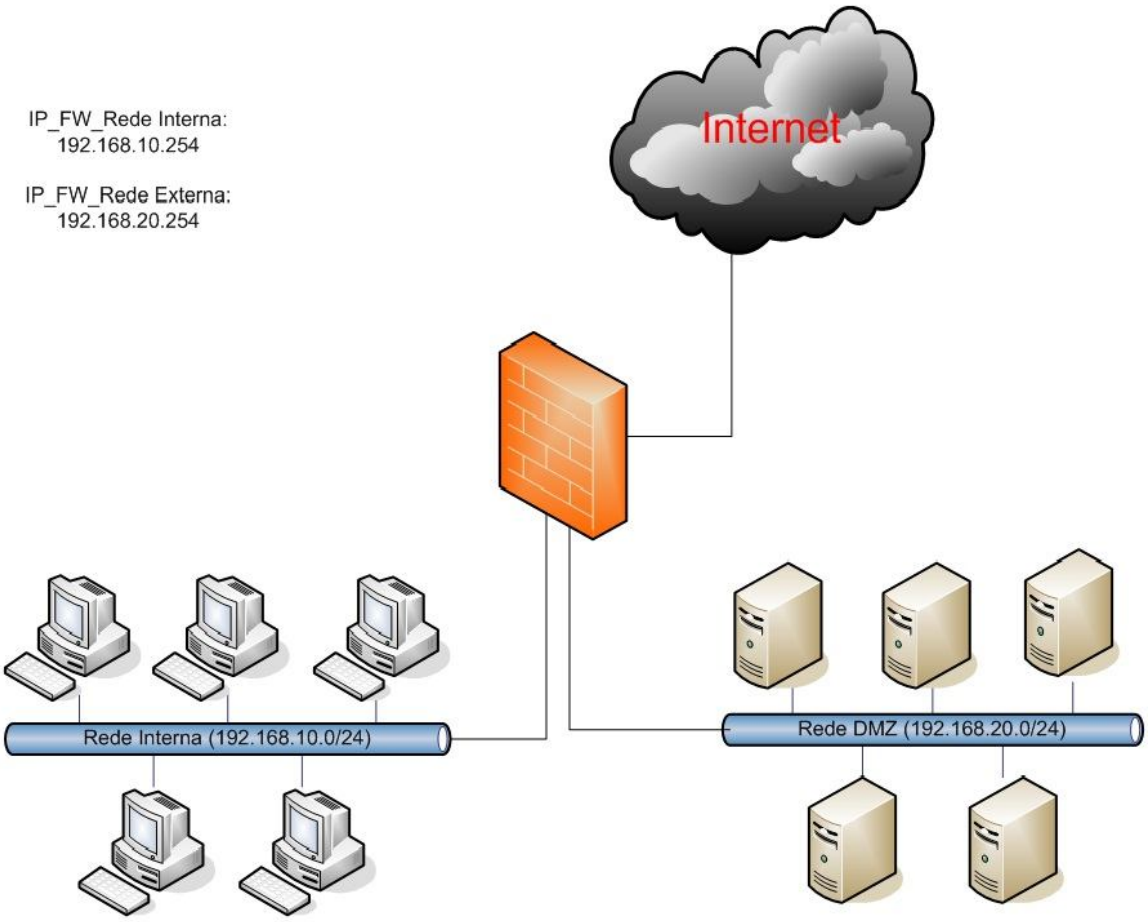


Diagrama 1: Diagrama de Estrutura de Rede

Fonte: Autoria Própria

Conforme o diagrama mostra o Firewall que será o equipamento que terá o contato direto com a rede externa (Internet); possui também duas redes distintas, uma destinada as estações de trabalho utilizadas pelos usuários denominada Rede Interna e a outra denominada Rede DMZ que consiste da rede utilizada pelos servidores adotados pela empresa, como por exemplo (Proxy, Arquivos, Domínio, E-mail), todas as conexões serão gerenciadas pelo Firewall.

5.3 PROXY (SQUID)

Utiliza-se esta ferramenta para efetuar o controle ao acesso à Internet dos usuários, escolhi como padrão deixar todos os sites bloqueados através da ACL:

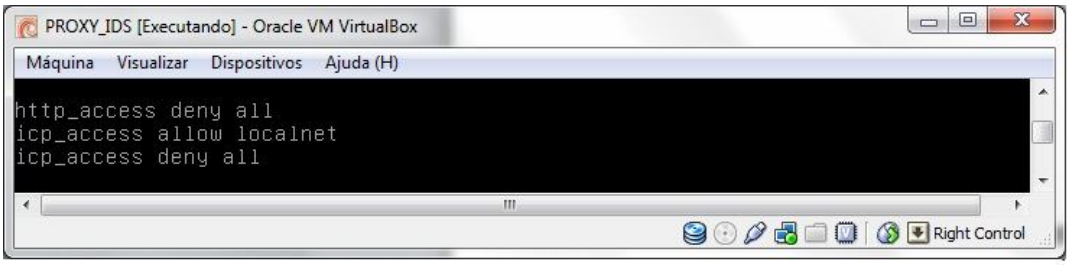


Figura 4: Configuração de acesso negado as url's

Fonte: Configuração Máquina Virtual

Conforme a necessidade de acesso, precisa-se configurar os sites em que seja possível a navegação através de um arquivo chamado LIBERADOS.TXT e para que seja possível esta liberação é necessário as seguintes configurações nas regras no squid.conf conforme mostrado abaixo.

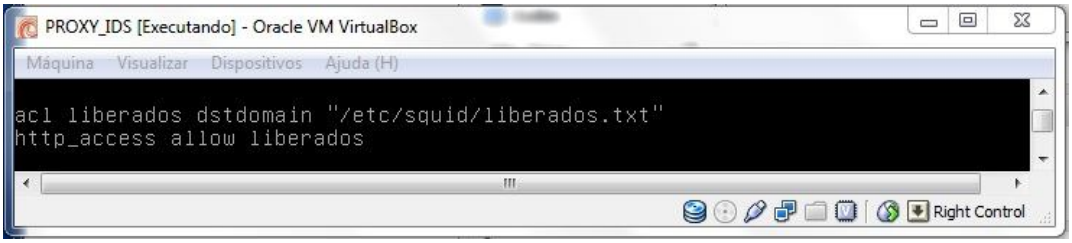


Figura 5: Configuração de acesso liberados as url's

Fonte: Configuração Máquina Virtual

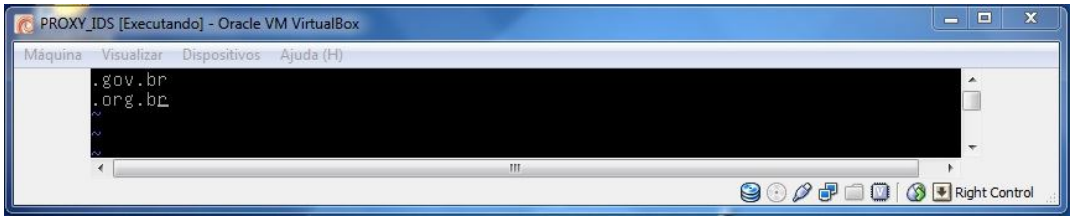


Figura 6: Arquivo liberados.txt

Fonte: Configuração Máquina Virtual

Neste caso somente para efeitos de laboratório deixa-se configurado como liberados somente os sites (.GOV.BR e .ORG.BR) todos os outros continuam sem acesso; outra maneira que irá aplicar para efetuar a liberação de acesso a internet será através do arquivo HOSTLIBERADO.TXT, onde neste serão determinados as estações que terão o acesso completamente liberado do acesso a internet; conforme abaixo:

Figura 7: Configuração de acesso hosts liberados.

Fonte: Configuração Máquina Virtual

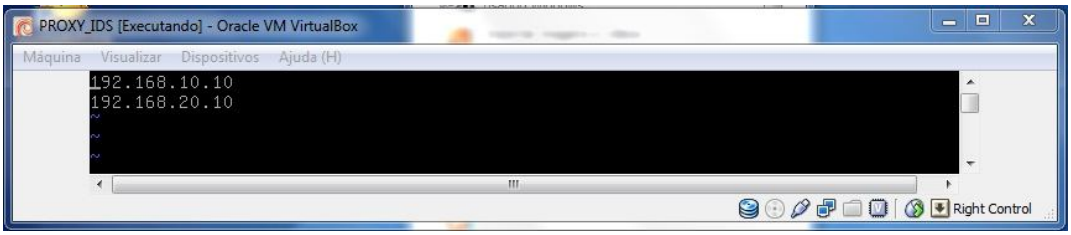


Figura 8: Arquivo hostliberado.txt

Fonte: Configuração Máquina Virtual

Estas serão as principais configurações que é pretende-se aplicar nesta solução, outra configuração que será aplicada é a utilização do Proxy de maneira transparente ao usuário, excluindo assim a necessidade da configuração manual em cada estação; esta configuração será efetuada no Firewall definindo a rota de saída passar pelo endereço do Proxy previamente e somente então acessar o url desejado; utilizando o SARG ferramenta que torna possível a demonstração visual dos acessos efetuados pelas estações, serão demonstrados relatórios dos endereços acessados para um melhor gerenciamento.

Nesta máquina virtual também estará configurado o servidor de IDS (Snort) que irá auxiliar a detectar possíveis acessos indevidos para poder verificar se a solução de segurança está atendendo ao proposto.

5.4 FIREWALL (IPTABLES)

Conforme explicado anteriormente, é utilizado o tipo de Híbrido instalado em uma nova maquina virtual, aplica-se nesta as configurações de firewall utilizando IPTABLES, aqui irá definir a política padrão como DROP (rejeitando todas as conexões) e liberando os acessos a portas de serviços que a empresa ache necessário, neste caso, vou deixar liberadas as portas 80(HTTP), 25(SMTP), 443(HTTPS), estes, serão necessários para a navegação via internet e para envio de e-mail via cliente de e-mail (Mozilla ThunderBird, Microsoft Outlook, etc.); para os serviços de entrada na rede pretendo deixar o mínimo de recursos disponíveis liberados um serviço que tenho de deixar liberado é o recebimento de e-mails na porta 110 (POP3). Outra configuração que estará contida no servidor firewall é função de NAT, como neste modelo de solução desejada é que ele, o firewall, esteja em contato com a internet.

Abaixo irá demonstrar quais serão as configurações definidas no firewall:

```
#Comando para limpar possíveis configurações já aplicadas

iptables –F

#Comando utilizado para limpar configurações de NAT

iptables -t nat -F

#Este comando é utilizado para se poder executar as funções de roteamento dentro do servido Firewall

echo 1 > /proc/sys/net/ipv4/ip_forward

#As Linhas abaixo são utilizadas para definir a saída das redes (interna e DMZ) para internet com o endereço do Firewall

iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

#Definindo a rota para ser utilizado proxy transparente

iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to 192.168.20.10:3128
```

#Agora estas definições serão utilizadas para tornar a regra padrão para bloquear todas as requisições.

iptables -P INPUT DROP

iptables -P OUTPUT DROP

iptables -P FORWARD DROP

#Regras para tabela INPUT

#Libera os pacotes vindos das redes (DMZ e INTERNA) e da interface de loopback

iptables -A INPUT -i lo -j ACCEPT

iptables -A INPUT -i 192.168.10.0/24 -j ACCEPT

iptables -A INPUT -i 192.168.20.0/24 -j ACCEPT

#Libera o acesso SSH ao servidor

iptables -A INPUT -p tcp --dport 22 -j ACCEPT

#Libera o acesso a porta do servidor squid para rede interna

iptables -A INPUT -p tcp --dport 3128 -j ACCEPT

#Libera as portas 80 (HTTP) e 53 (DNS) utilizadas para navegação

iptables -A INPUT -p tcp -m multiport --dport 80,53 -j ACCEPT

#Regras para Tabela OUTPUT

#Libera o DNS para o localhost

iptables -A OUTPUT -p tcp --dport 53 -j ACCEPT

iptables -A OUTPUT -p udp --dport 53 -j ACCEPT

#Libera as portas 80 (HTTP) e 53 (DNS) utilizadas para navegação

iptables -A OUTPUT -p tcp -m multiport --dport 80,53 -j ACCEPT

#Regras para tabela FORWARD

#Regra para o recebimento de email.

iptables -A FORWARD -d <Endereco Servidor de Envio> -p tcp -m tcp --dport 25 -j ACCEPT

iptables -A FORWARD -d <Endereco Servidor de recebimento> -p tcp -m tcp --dport 110 -j ACCEPT

#Regras para o retorno de email.

iptables -A FORWARD -s <Endereco Servidor de Envio> -p tcp -m tcp --sport 25 -j ACCEPT

iptables -A FORWARD -s <Endereco Servidor de recebimento> -p tcp -m tcp --sport 110 -j ACCEPT

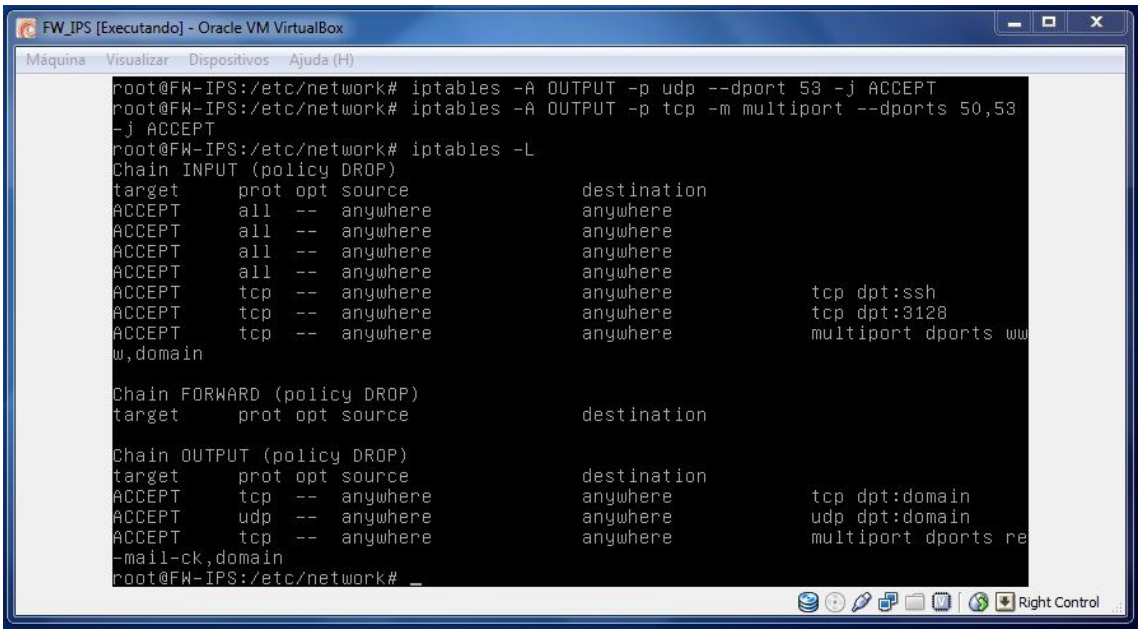


Figura 8: Configurações Firewall

Fonte: Configuração Máquina Virtual

6 CONCLUSÃO

A utilização do meio eletrônico tornou necessária a mudança de diversos hábitos dentro das empresas, o cuidado com a segurança das informações tornou-se um item imprescindível para qualquer tipo de organização, uma vez que os serviços executados nas empresas se encontrão no meio eletrônico; a comunicação entre as organizações utiliza o meio eletrônico através de e-mail; serviços bancários hoje em dia são praticamente todos executados via internet, ou seja, estará ficando totalmente dependentes do meio virtual para executar as tarefas diárias.

Com este novo ambiente que se criou, as organizações tiveram de adaptar suas estruturas para que as informações que ela gera sejam protegidas de acessos indevidos, seja pelo próprio funcionário da empresa ou por uma pessoa que encontrou alguma vulnerabilidade na rede da organização e coletou estas informações sem autorização.

A ferramenta que foi citada neste trabalho teve como principal foco o desenvolvimento uma solução de segurança para as informações de uma pequena organização, pois utiliza ferramentas que não geram um custo grande e possibilitam controlar diversos tipos de ameaças e ainda utilizando um número reduzido de equipamentos físicos, diminuindo ainda mais o custo para implantação da solução.

As principais dificuldades para implantação desta solução é a resistência das organizações em não perceber os riscos que a empresa sofre disponibilizando serviços na internet pensando que nunca vai acontecer nada com a sua empresa quando nem sempre isso se torna verdadeiro; mas o principal desafio é o treinamento do usuário este é ainda mais complicado de fazê-lo entender quanto importante são os cuidados que se deve adotar para utilização dos recursos eletrônicos disponibilizados pela empresa, geralmente os problemas enfrentados pelas organizações são decorrentes dos usuários sejam por engenharia social ou pela ingenuidade do usuário em comentar assuntos referentes ao seu trabalho.

7 REFERÊNCIAS

MARCELO, Antonio. Squid: configurando o Proxy para Linux. 4. ed. atual. Rio de Janeiro: Brasport, 2005. 75 p. ISBN 85-7452-213-9

Urubatan Neto. Dominando Linux Firewall Iptables. Rio de Janeiro: Ciência Moderna, 2004. 98 p. ISBN 8573933208

Anonymous; tradução de Edson Furmankiewicz e Joana Figueiredo. Segurança Máxima para Linux. Rio de Janeiro: Campus, 2000. 761 p. ISBN85-352-0627-2.

Mendes, Douglas Rocha, Redes de computadores 1.Edição Editora Novatec, Rio de Janeiro 2009.

NAKAMURA, Emílio Tissato e GEUS, Paulo Lício de: Segurança de Redes em Ambientes Cooperativos. Berkeley 2002

TANENBAUM, Andrew S. Redes de Computadores. 4 Ed. Editora Campus 2010. 632p.

STALLINGS, William. Redes e Sistemas de Comunicação de Dados. Editora Campus 2005. 460p.

MORAES, Alexandre Fernandes de. Segurança em Redes. São Paulo: Érica, 2010. 264 p. ISBN978-85-365-0325-7

ZWICKY, ELIZABETH D.; Construindo Firewalls para a Internet. 2ª ed. Rio deJaneiro, Editora Campus,2001.

CARISSIMI, Alexandre. Virtualização: da teoria a soluções. Simpósio Brasileiro de Redes de Computadores 2008, p.173 – 207.

http://cartilha.cert.br/download/; acessado em outubro de 2011.

http://www.cert.br/docs/seg-adm-redes/; acessado em outubro de 2011.

http://www.mlaureano.org/guias_tutoriais/GuiaInstSquid.htm; acessado em fevereiro de 2012.

http://www.squid-cache.org/; acessado em janeiro de 2012.

http://www.vmware.com/br/virtualization/; acessado em janeiro de 2012.

http://www.gta.ufrj.br/grad/09_1/versao-final/virtualizacao/referencias.html; acessado em março de 2012.

http://vembajr.wordpress.com/category/wake-up-africa/; acessado em abril de 2012.

http://www.hardware.com.br/artigos/ferramentas-virtualizacao/; acessado em abril de 2012.