UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ESPECIALIZAÇÃO EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDES

ALEXANDRE BATISTA SAMPAIO

IMPLANTAÇÃO DE POLÍTICAS DE SEGURANÇA EM REDES DE COMPUTADORES COM PIX FIREWALL

MONOGRAFIA DE ESPECIALIZAÇÃO

CURITIBA
2011

ALEXANDRE BATISTA SAMPAIO

IMPLANTAÇÃO DE POLÍTICAS DE SEGURANÇA EM REDES DE COMPUTADORES COM PIX FIREWALL

Monografia apresentada como requisito parcial à obtenção do grau de Especialista em Configuração E Gerenciamento de Servidores E Equipamentos de Redes, do Departamento Acadêmico de Eletrônica, da Universidade Tecnológica Federal do Paraná.

Orientador: Prof. Dr. Kleber Kendy Horikawa Nabas

CURITIBA
2011

RESUMO

SAMPAIO, Alexandre Batista. **Implantação de políticas de segurança em redes de computadores com PIX Firewall**. 2011. 35 folhas. Monografia (Curso de Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes) - Universidade Tecnológica Federal do Paraná. Curitiba, 2011.

Este trabalho pretende avaliar quais as principais políticas de segurança a serem cultivadas em uma rede de computadores e demonstrar como elas devem ser aplicadas utilizando a tecnologia da corporação Cisco conhecida como PIX Firewall. Em um ambiente virtual serão apresentados os passos para a elaboração de algumas configurações, e no fim deste projeto serão dispostas as análises recolhidas durante o processo de virtualização do sistema proposto e compara-lo a outras soluções em uma adjacência como um todo. Poderemos observar o alto nível de desempenho oferecido pela solução PIX Firewall, que detém grande estabilidade e ao mesmo tempo uma vasta gama de recursos.

Palavras-chave: Políticas de Segurança. Redes de Computadores. PIX. *Firewall*. Cisco

SUMÁRIO

1 INTRODUÇÃO

Esta seção tratará sobre o tema, o problema e premissas, a delimitação da pesquisa, os objetivos, a justificativa e os procedimentos metodológicos.

1.1 TEMA

Como introdução, pode-se aludir que Firewall é um *software* com o principal objetivo de filtrar pacotes que trafegam de um *host*/rede a outro. O *Private Internet Exchange* (PIX) da Cisco, por sua vez possui o mesmo conceito, adicionado de alguns recursos que auxiliam no gerenciamento e na administração das políticas de segurança de uma rede.

Para delimitação da pesquisa, quanto aos métodos e processos de simulação e desenvolvimento do tema, o objeto de exame será exclusivamente um Firewall. Outros serviços como *Virtual Private Network* (VPN), Proxy e ferramentas de criptografia, até poderão ser citados, mas como este estudo não se aplica a isso, não serão explicados.

1.2 PROBLEMA E PREMISSAS

Nota-se que o alcance a materiais de consulta sobre temas específicos referentes à aplicação e gerenciamento da segurança em redes de computadores é escasso. Em geral, esses recursos são estrangeiros e, por sua vez, comumente, possuem documentações apenas no dialeto nativo, dificultando ainda mais aos pesquisadores a obtenção de informações exclusivas. Outro aspecto problemático origina-se na falta de recursos triviais para o meio acadêmico, enfatizando a idéia que se aplica a exclusividade, a qual faz com que mesmo comercialmente, seja enredada a obtenção das informações necessárias para estudos e pesquisas.

Devido a isso, devem ser desenvolvidos materiais que explorem conceitos particulares, de forma a globalizar as informações e difundir o conhecimento específico.

1.3 OBJETIVOS

Esta seção tratará dos objetivos geral e específicos.

1.3.1 Objetivo Geral

Demonstrar como implantar as políticas de segurança em uma rede de computadores utilizando a solução PIX Firewall da Cisco.

1.3.2 Objetivos Específicos

- Analisar as regras básicas para implantação de um *firewall* em uma rede de computadores;
- Simular ambientes de redes utilizando a solução PIX Firewall;
- Definir métodos e processos para implantação e gerenciamento de políticas de segurança em um firewall e
- Avaliar as vantagens e desvantagens da solução PIX Firewall.

1.4 JUSTIFICATIVA

Devido à crescente globalização que amplia as conexões entre todo o mundo, a segurança das informações é algo que deve ser cada vez mais aprimorada, portanto este trabalho justifica-se por prover conhecimentos básicos, contudo específicos, de uma ferramenta que disponha de ótimos recursos para garantir a segurança de uma rede de computadores.

1.5 PROCEDIMENTOS METODOLÓGICOS

Fazer uma revisão bibliográfica a respeito de segurança das informações, especificamente sobre *firewall*. O método de pesquisa será de caráter exploratório experimental cujo objetivo é reunir informações e explorar os recursos que a solução PIX Firewall oferece, utilizando livros, artigos, sítios, entre outros.

1.6 EMBASAMENTO TEÓRICO

Segundo Urubatan Neto (2004), a Bell Labs é a empresa que desenvolveu o primeiro *Firewall* do mundo, solicitado pela AT&T por volta de 1980, o qual “foi desenvolvido com o intuito de filtrar todos os pacotes que saíssem e entrassem na rede corporativa” (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*. O *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.

O *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.

Já o *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).

Para falarmos sobre o PIX Firewall, é de estrema importância conhecer o propósito de *Adaptive Security Algorithm* (ASA - Algoritmo de Segurança Adaptativa). “O ASA é uma abordagem completa para segurança. Cada pacote de entrada é verificado pelo ASA e pelas informações de estado de conexão na memória do PIX FIREWALL.” (Cisco Systems, 2000, p. 2-3, tradução nossa).

Para encerrar a exposição do embasamento teórico, atendendo ao objetivo específico de analisar as regras básicas para implantação de um *firewall* em uma

rede de computadores, a pesquisa conta com a contribuição dos autores Urubatan Neto (2004) e Alexandre Freire (2004), e da instituição Cisco Systems, Inc.

1.7 ESTRUTURA

Este trabalho será constituído por uma estrutura composta por 6 capítulos. Na introdução, capítulo 1, serão apresentados o tema da pesquisa e seus delineamentos, seguidos pela apresentação do problema e das premissas, dos objetivos, das justificativas, dos procedimentos metodológicos, do embasamento teórico e da estrutura da dissertação, aqui exposta. Os capítulos 2 e 3 concentrarão a fundamentação teórica da pesquisa, os principais aspectos de um *Firewall*, especialmente sobre o PIX Firewall, e suas delimitações como também os processos necessários para execução de testes em um ambiente simulado.

2 POLÍTICAS DE SEGURANÇA EM UM FIREWALL

Política de segurança, em geral, é um conjunto de regras que definem os mecanismos de segurança a serem implementados em uma organização, e como eles devem ser configurados e gerenciados. Toda política de segurança deve estar de acordo com as adaptações da organização e serem seguidas por todos os usuários dos meios tecnológicos que a política se refere. Uma política de segurança como qualquer outro tipo de política, deve seguir conceitos éticos e legais que não interfiram nas relações entre colaborador e companhia.

Segundo Alexandre 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.

Para uma boa política de segurança, Freire (2004) recomendou o bloqueio de alguns serviços que podem aumentar o nível de segurança do perímetro de uma corporação contra ataques procedentes da Internet:

Segundo Freire (2004), devemos bloquear pacotes originários de endereços inválidos previstos em RFC.

> Executar o bloqueio de endereços forjados ("*spoofed*" *addresses*). Pacotes originários do mundo exterior com origem de redes privadas (endereços internos previstos na RFC 1918 e rede 127) devem ser bloqueados e desconsiderados como tráfego de rede válido quando trafegando pelo meio público Internet. A importância do bloqueio de pacotes recebidos da Internet e que possuem endereço de origem de redes privadas ou endereços de *loopback*, reside em auxiliar na proteção contra o envio de pacotes forjados (*spoofing*). (FREIRE, 2004).

Freire (2004) aconselha bloquear serviços de Login como Telnet (porta 23 do TCP), SSH (porta 22 do TCP), FTP (porta 21 do TCP), NetBIOS (porta 139 do TCP) e Rlogin (da porta 512 do TCP até a porta 514 do TCP).

Como Telnet é utilizado para acesso remoto via terminal, onde informações como usuário, senha e dados, são exibidas abertamente e desprotegidas na rede por não possuir padrões de criptografia, “estas informações automaticamente ficam expostas e passíveis de interceptação através da utilização de *sniffers*” (FREIRE, 2004).

> Telnet também é vulnerável ao que chamamos de "captura de sessão" (*session hijacking*), permitindo a usuários remotos total controle sob sessões onde através da captura de uma sessão, é possível o comprometimento de um sistema diretamente através do Shell do sistema operacional. (FREIRE, 2004).

O serviço de FTP é exclusivamente utilizado para a transferência de arquivos entre *hosts*. “O grande problema diagnosticado em relação ao FTP é a má configuração das permissões de acesso aos diretórios publicáveis” (FREIRE, 2004).

> Uma má configuração permite a modificação de arquivos para exploração de serviços como *rsh* e *rexec*, ou download do arquivo de senhas de um servidor, permitindo acesso a demais áreas criticas ou até mesmo a oportunidade de utilização do servidor de FTP de uma corporação como repositório de programas piratas e imagens. Assim como o Telnet, uma sessão de FTP pode ser sequestrada e a informação, que também é enviada em claro, pode ser alvo de práticas de *sniffing*. (FREIRE, 2004).

Rlogin e semelhantes se responsabilizam por estabelecer confiança entre dois hosts a partir de um endereço de origem. “Estes serviços significam um grande risco a sistemas Unix porque eles são utilizados para o processo de *login* automático através da rede com o objetivo de execução de comandos em sistemas remotos” (FREIRE, 2004).

> As informações também trafegam em claro, proporcionando captura através de *sniffing*. Em muitas ocasiões, o servidor de FTP é porta de entrada para que invasores preparem o acesso remoto ao Shell do sistema operacional, a partir da manipulação dos arquivos de controle como o /etc/hosts.equiv e .rhosts. (FREIRE, 2004).

SSH pode ser utilizado para substituir serviços de emulação de terminal, como Telnet, e transferência de arquivos, como FTP.

> A implementação do SSH garante segurança adicional na medida em que os dados de emulação de terminal não são transferidos em claro pela rede, assim como as transferências de arquivos que, a partir da utilização do subsistema de FTP do *daemon* de SSH, garante a proteção das informações que são enviadas ou recebidas com camada de criptografia. (FREIRE, 2004).

Segundo Freire (2004) a utilização do SSH requer cuidados, tanto porque o mesmo é alvo de ataques, principalmente do tipo *buffer overflow*.

> Em implementações antigas do *daemon* de SSH, um buffer overflow proporcionava ao invasor a exploração de uma porta para acesso privilegiado no Shell do sistema operacional, assim como o famoso ataque *Man in the middle*, que pode ser resumido como um problema de educação na distribuição das chaves de criptografia utilizadas para estabelecer a autenticação de um usuário perante a um servidor rodando o *daemon* de SSH. (FREIRE, 2004).

Segundo Freire (2004) assim como qualquer outro emulador, é muito importante que o serviço de SSH esteja sempre atualizado com a versão mais recente do produto “para que o acesso à emulação de terminal ou transferência de arquivos não seja comprometido ou sirva de porta de entrada informal para uma possível invasão do sistema operacional” (FREIRE, 2004).

Freire (2004) também recomenda o bloqueio dos serviços Portmap/RPCBind (porta 111 do TCP e do UDP), NFS (porta 2049 do TCP e do UDP), Lockd (porta 4045 do TCP e do UDP).

Segundo Freire (2004) o serviço Portmap é responsável por manter o estado dos serviços de RPC (Remote Procedure Call). “Entenda-se por RPCBind o nome do Portmapper em sistemas utilizando TI-RPC” (FREIRE, 2004).

> Um invasor ao estabelecer conexão na porta 111 utilizando, por exemplo, o comando "rpcinfo", pode receber informações a respeito das aplicações registradas em um servidor. O comando chama a sub-rotina PMAPPROC_DUMP e exibe a listagem das portas utilizadas por cada programa RPC. É uma informação preciosa para o conhecimento dos processos e aplicações registradas em um sistema operacional Unix. (FREIRE, 2004).

O Network File System (NFS), permite que um host monte os arquivos do sistema em um servidor.

> Os principais problemas encontrados em um ambiente NFS são o IP *spoofing*, visto que o mesmo faz uso do endereçamento IP para controle de acesso e permissões para compartilhamento (*export*) de diretórios

> configurados de maneira incorreta, respectivamente. É muito comum que os administradores de ambientes Unix exportem, em um ambiente NFS, diretórios sem restrições de acesso, exportando diretórios inteiros como Read/Write para o que chamamos de "world". Assim sendo, qualquer cliente pode "montar" os filesystems exportados e acessar informações confidenciais que foram compartilhadas de maneira incorreta. (FREIRE, 2004).

Em conjunto ao NFS, Freire (2004) expõem que Lockd é um programa RPC utilizado para manipular e administrar solicitações de acesso a arquivos tanto localmente a partir do kernel, como remotamente de outro *lock daemon*.

> O processo relaciona-se ao NFS no que se diz respeito a responsabilidade de gerenciar a utilização de um recurso reservando acesso exclusivo ao mesmo (*locking*). Diversas implementações do Daemon Lockd estão vulneráveis a ataques do tipo *Denial Of Service*, comprometendo o acesso exclusivo e permitindo que outras estações transmitam comandos RPC ao NFS Server. (FREIRE, 2004).

Freire (2004) aconselha bloquear também as portas 135 (TCP e UDP), 138 (UDP), 139 (TCP) além da porta 445 (TCP e UDP), que são utilizadas pela interface de desenvolvimento de aplicação NetBios.

> O tráfego de *username*/senhas em uma rede Windows NT é vulnerável a *sniffers* e *crackers*... Diversas ferramentas existentes hoje, como por exemplo, o NAT (*Netbios Auditing Tool*), permitem a um invasor descobrir senhas e acessar recursos em um servidor, existindo a possibilidade de acesso a demais domínios pertencentes ao sistema através de relação de confiança (*trust relationship*) da rede Microsoft. O tráfego Netbios permite através de um acesso anônimo, a enumeração de recursos, contras, configuração do sistema e chaves do registro. (FREIRE, 2004).

Outra recomendação por parte de Freire (2004) é o bloqueio de todas as portas do intervalo entre 6000 e 6255 do TCP, as quais são empregadas por sistemas X-Windows. Segundo Freire (2004), basicamente existem dois níveis de proteção agregados à funcionalidades do X-Window System. “O Xhost utiliza endereçamento IP para restringir quais atividades são autorizadas. O Xauth, proporciona proteção semelhante, mas sua utilização baseia-se no uso de uma *string* secreta, a qual denominamos *magic cookie*” (FERIRE, 2004).

> Existem muitos artifícios a serem explorados por um invasor no que se diz respeito à invasão a um X11 Server. Podemos destacar a possibilidade de captura de *screen*, redirecionamento do *display*, *mouse* e teclado para a entrada de comandos arbitrários e o estabelecimento de sessão remota para execução de comandos no host remoto. Algumas versões ainda são vulneráveis a ataques do tipo *buffer overflow*, permitindo, por exemplo, a um

> usuário na Internet, ter pleno acesso como usuário *root* ao *shell* do sistema operacional, condicionando uma situação de total domínio e comprometimento do host. (FREIRE, 2004).

Freire (2004) aconselha ainda o bloqueio do serviço de resolução de nomes (DNS, porta 53 do UDP) para todas as máquinas que não são servidores de DNS, e a Transferência de Zona (porta 53 do TCP) para todos os computadores que não são servidores de DNS secundários. “Um invasor pode poluir o cache de um DNS remoto provendo informações erradas sobre um *hostname*, direcionando o acesso a este *hostname* para um *site* de pornografia”, ou a um por exemplo. (FREIRE, 2004).

Segundo Freire (2004), após o *Active Directory* ter se tornado um repositório de objetos unificado, informações importantes sobre usuários podem ser extraídas rapidamente através de *queries* a arvore de diretórios.

> Diretórios implementando LDAP podem conter informações particulares de funcionários e informações sobre a organização. Um invasor pode explorar vulnerabilidades associadas ao LDAP, em sua maioria *buffer overflows*, para modificar informações armazenadas pelo mesmo. Outra grande preocupação é o receio de um *Denial Of Service* no serviço de diretórios indisponibilizando procedimentos de autenticação. (FREIRE, 2004).

Freire (2004) também recomenda o bloqueio de SMTP (porta 25 do TCP) para todas as máquinas que não são *relays* externos, POP (portas 109 e 110 do TCP) e IMAP (porta 143 do TCP).

Devido à grande utilização do protocolo SMTP, “é natural que o mesmo tenha uma grande incidência de consultas por invasores que identificam tipos diferentes de tráfego que um ambiente alvo possa disponibilizar” (FREIRE, 2004).

> SMTP não proporciona confidencialidade e autenticação. O mesmo é vulnerável a *sniffing* e modificações de *host/username*. SMTP também pode ser alvo de *Denial Of Service*, ataques de *buffer overflow* ou mesmo de consultas importantes que podem ser realizadas através de comandos suportados pelo servidor de SMTP e que permitem, por exemplo, a verificação de usuários existentes no sistema operacional (procedimento útil para viabilizar ataques do tipo *brute force / password guessing*). (FREIRE, 2004).

Freire (2004) afirma que POP não deve ser permitido para nenhum *host* externo da rede, caso a Política de Segurança da mesma preze por esta recomendação.

> Como o POP3 transmite senhas em claro, invasores podem descobrir senhas a partir de análise de tráfego do barramento com a utilização de *sniffers*, acessar caixas postais e muitas vezes, replicar as senhas encontradas no acesso a um serviço de e-mail externo para recursos internos da corporação. (FREIRE, 2004).

De mesmo modo, “o *Internet Message Access Protocol* (IMAP), segue o mesmo conceito de vulnerabilidade, caracterizando-se por ser vulnerável a *sniffing*” (FREIRE, 2004).

Freire (2004) ainda recomenda a restrição de acesso à serviços HTTP somente aos servidores que necessitam prover serviços web, limitando seus acessos somente às portas 80 e 443. “Limitar acesso somente aos servidores que necessitam prover serviços Internet previne possíveis invasões a servidores que não foram preparados ou devidamente configurados para exercer esta função” (FREIRE, 2004).

> Outro aspecto importante é eliminar os servidores que "escutam" em portas altas. É muito importante para organização e controle do tráfego HTTP, que o serviço seja limitado às portas 80 e/ou 443. Esta medida tem o objetivo de prevenir buracos abertos no Firewall através da abertura de portas chamadas efêmeras, ou portas altas (portas acima de 1024). (FREIRE, 2004).

Outra recomendação feita por Freire (2004) é o bloqueio do tráfego direcionado a portas abaixo das portas 20 do TCP e do UDP, assim como serviço *Time* (porta 37 do TCP e do UDP). “Muitos dos chamados *Small Services* podem levar um servidor ou equipamento de conectividade a morrer em um ataque *Denial Of Service*. Estão compreendidos no grupo *Small Services* os serviços *echo*, *chargen*, *discard*, e *daytime*” (FREIRE, 2004).

Segundo Freire (2004), o serviço *Time* só deve ser provido com um serviço interno e não deve ser aceito de uma origem não confiável.

Em seu artigo, Freire (2004) explica que é muito comum a utilização dos serviços *Chargen* e *Echo* em combinação para forçar a lentidão de um *host* ou até um *crash* no sistema operacional do mesmo.

> Através do *spoofing* de uma conexão *chargen* para um serviço *echo*, é possível combinar os dois serviços em um cenário de uma "conversa eterna", onde os caracteres enviados entrarão em *looping* toda vez que forem recebidos e impressos na tela pelo serviço *Echo*. (FREIRE, 2004).

Freire (2004) afirma que ninguém em vias normais utiliza os *Small Services* e que eles existem somente para permitir aos invasores um canal para obtenção de informações adicionais para possibilitar uma invasão através da utilização de *exploits*.

Outra sugestão de Freire (2004) é o bloqueio do tráfego direcionado à TFTP (porta 69 do UDP). Segundo Freire, o TFTP deve ser barrado, e muitos dos motivos podem ser associados ao FTP, mas o principal motivo, é que o mesmo não proporciona nenhuma segurança, visto que não é necessário nenhum procedimento de autenticação para transferência das informações.

> Se incorretamente implementado, o TFTP permitirá que um usuário execute o download de qualquer arquivo de um determinado host. Muitos são os casos de arquivos inteiros de configurações importantes e até arquivos de senhas de sistemas Unix/Linux que são obtidos por invasores a partir da utilização do TFTP em ambientes onde o serviço encontra-se ativo e mal configurado. (FREIRE, 2004).

Para Freire (2004), todo tráfego direcionado a porta 79 do TCP deve ser bloqueado, pois o "serviço *Finger* permite a obtenção de informações preciosas para invasores em um estudo inicial de um servidor ou ambiente de rede" (FREIRE, 2004)

> Através do FINGER é possível identificar o nome real de usuários, respectivos números de telefone, *home directory* dos usuários, *shell* utilizado para o procedimento de *login*, tempo de conexão do usuário, data que o usuário leu o último e-mail, assim como host de procedência de conexão. (FREIRE, 2004).

Com essas informações, um invasor pode executar tentativas de acesso por força bruta ou ainda adimplir ataques de engenharia social.

Freire (2004) sugere ainda que o tráfego referente ao serviço *Network News Transport Protocol* (NNTP), o qual utiliza a porta 119 do TCP, seja bloqueado.

> NNTP utiliza listas de controle de acesso que são baseadas em *hostnames*. O protocolo é vulnerável a IP *Spoofing*. Um invasor pode ter acesso a um NNTP Server e verificar informações confidenciais postadas em listas de discussão específicas. (FREIRE, 2004).

Visto que uma política de segurança não se trata somente da segurança das informações, mas da rede como um todo e da sua disponibilidade, o NNTP possui um volume de tráfego consideravelmente alto, o que pode comprometer a banda de

internet, o que auxilia na queda do desempenho da rede e consequentemente sua degradação de disponibilidade.

Freire (2004) indica a interceptação do tráfego direcionado à porta 123 do TCP, a qual é responsável pelo serviço *Network Time Protocol* (NTP), e que por sua vez deve ser bloqueado pelos mesmos motivos do serviço *Time*.

> O tráfego NTP pode ser forjado e utilizado como técnica para tentativa de alteração da data e hora em um sistema antes de sua invasão. Desta maneira, os *logs* de acesso durante uma invasão indicariam informações com data e hora diferentes em relação ao tempo de ocorrência verdadeiro de um incidente, inviabilizando assim, a possibilidade de comparar os *logs* de um servidor invadido com outros logs de dispositivos de segurança espalhados pela rede. (FREIRE, 2004).

O bloqueio do tráfego direcionado à porta 515 do TCP, que é utilizada pelo protocolo de impressão de sistemas Unix (LPD), é recomendado por Freire (2004), que indica o LPD como vulnerável a ataques de *buffer overflow*. Freire afirma também que LPD possui problemas similares a outros serviços que utilizam o *stack* TCP/IP, como *Denial Of Service* e IP *spoofing* através da simulação de *jobs* de impressão falsos.

Em seu artigo, Freire (2004) também expõe a necessidade de bloquear a porta 514 do UDP, a qual é responsável pelo serviço SYSLOG.

> Desde que a maioria dos servidores de SYSLOG aceite tráfego não autenticado, é possível a exploração de entradas falsas nos registros de log a partir de um invasor. Mensagens falsas podem ser utilizadas para gerar um ataque do tipo *Denial Of Service*. Outro ponto importante é que informações críticas de hosts podem ser obtidas a partir da análise do tráfego SYSLOG. (FREIRE, 2004).

Freire (2004) recomenda ainda o bloqueio do tráfego referente ao protocolo *Simple Network Management Protocol* (SNMP), que atua nas portas 161 e 162, ambas do TCP e do UDP, pois é um serviço comumente identificado e explorado por invasores. A atração dos invasores pelo SNMP é o fato dele permitir o gerenciamento remoto de equipamentos de rede que variam desde roteadores e impressoras a servidores e computadores clientes.

“A maioria das implementações de SNMP em ambiente de rede utiliza a *string public* como mecanismo de autenticação de seus dispositivos. Isso permite conexão sem restrições de qualquer origem para administração” (FREIRE, 2004).

> Tráfego SNMP é passível de *sniffing* e pode revelar informações a respeito da estrutura de um ambiente de rede, assim como de sistemas e dispositivos. Invasores utilizam essas informações para escolher alvos e planejar ataques. Através da exploração da *community* "*public*", os invasores podem reconfigurar e até desligar equipamentos. (FREIRE, 2004).

Outra Recomendação de Freire (2004) é o bloqueio do tráfego direcionado ao *Border Gateway Protocol* (BGP), que atua na porta 179 do TCP.

> Em ambientes de rede onde o roteador de borda não esteja conectado a uma infraestrutura BGP, é aconselhável o bloqueio de tráfego BGP a partir do perímetro da rede, visto que o BGP é vulnerável a ataques do tipo *SYN Flood* e a ataques TCP com *flag* RST que tem como objetivo reiniciar conexões estabelecidas a servidores. (FREIRE, 2004).

Freire (2004) Também aconselha o bloqueio do protocolo SOCKS, que opera na porta 1080 do TCP.

> Como SOCKS é passível de vulnerabilidades que permitem ataques do tipo *Denial of Service*, assim como *buffer overflows*, caso seja necessária a utilização do mesmo é de extrema importância revisar as regras do sistema de Firewall para especificar explicitamente, o máximo possível, a origem e o destino de tráfego. (FREIRE, 2004).

É muito importante dar atenção a isto, pois uma falha na configuração pode liberar acessos externos indevidos, como a um servidor DNS ou a um servidor de Proxy.

Em seu artigo, Freire (2004) também expõe a necessidade de bloquear o *Internet Control Message Protocol* (ICMP), ou seja, impedir *Incoming Echo Request* (*ping* e *Windows Traceroute*), *Outgoing Echo Replies*, *time exceeded* e mensagens *unreachable*. Pois “ao invés da concepção de transportar dados, o protocolo pode ser utilizado por invasores para levantar informações do ambiente” (FREIRE, 2004).

Devido o ICMP *echo request* ser um dos métodos mais utilizados para mapeamento de redes, Freire (2004) aponta como grande importância restringir o *echo request* quando o mesmo é solicitado a partir da Internet com destino à rede.

> O famoso ataque de fragmentação "*Ping of Death*", utiliza pacotes ICMP fragmentados para causar ataque do tipo *Denial Of Service* através da técnica de criar pacotes IP que excedem a especificação de 65,535 bytes de dados. Este ataque resulta, muitas vezes, em *crash* ou congelamento do host. Além do *Ping of Death*, um invasor pode obter informações preciosas através da análise das mensagens ICMP e utilizar o protocolo para a técnica de ataques do tipo *Smurf* ou *Loki*. (FREIRE, 2004).

Todavia, é importante destacar que uma boa política de segurança aplicada em um *firewall* não se refere apenas a bloqueio de portas e serviços, e sim a um conjunto de regras e métodos que devem garantir tanto a segurança quanto a disponibilidade das informações, ou seja, usuários, senhas, permissões, serviços, entre outros recursos, devem ser cuidadosamente elaborados e configurados para que não haja dificuldades em garantir, de forma adequada, as políticas estabelecidas para a segurança da rede.

3 PIX FIREWALL

Segundo a Cisco Systems (2003), o PIX Firewall basicamente protege uma rede interna de acessos não autorizados pelos usuários em uma rede externa. “A maioria dos modelos PIX Firewall podem, opcionalmente, proteger um ou mais perímetros de redes, também conhecidos como zonas desmilitarizadas (DMZ)” (Cisco Systems, 2003, p. 1-2, tradução nossa).

Para usar um *firewall* de forma eficaz em uma rede, é necessária uma política de segurança que garanta que todo o tráfego da rede interna passe por meio do *firewall* para acessar a rede externa, da mesma forma, redes externas só podem conseguir acesso interno ao passarem pelo *firewall*.

O Anexo A mostra como um PIX Firewall protege uma rede, permitindo conexões de saída e assegurando o acesso à Internet.

> Dentro dessa arquitetura, o PIX Firewall forma a fronteira entre as redes protegidas e as redes desprotegidas. Todo o tráfego entre as redes protegida e desprotegida fluem através do firewall para manter a segurança. (Cisco Systems, 2003, p. 1-2, tradução nossa).

Com o PIX Firewall também é possível implementar políticas de segurança para a rede interna. “Normalmente, a rede interna é própria de uma rede da organização, ou intranet, e a rede externa é a Internet, porém o PIX Firewall também pode ser usado dentro de uma intranet para isolar ou proteger um grupo interno de usuários de outro” (Cisco Systems, 2003, p. 1-3, tradução nossa).

Segundo a Cisco Systems (2003) uma rede de perímetro pode ser configurada para ser tão segura quanto a rede interna ou com níveis de segurança diferentes. O Anexo B mostra como atribuimos níveis de segurança com valores numéricos para o PIX Firewall.

Os níveis de segurança do ASA identificam se uma interface é interna (confiável) ou externa (não confiável) em relação a outra interface. Para a Cisco Systems (2000) uma interface é considerada confiável em relação à outra interface, se seu nível de segurança for maior do que a das outras interfaces, e não é considerada confiável em relação à outra interface quando seu nivel de segurança for menor do que a outra interface.

> A regra principal para os níveis de segurança é que uma interface com um nível maior de segurança pode acessar uma interface com um nível menor de segurança. Por outro lado, uma interface com um nível menor de segurança não pode acessar uma interface com um nível maior de segurança sem uma condição. Níveis de segurança variam de 0 a 100. (Cisco Systems, 2000, p. 2-4, tradução nossa).

A Cisco Systems (2003) afirma que o ASA, sendo uma solução que executa abordagem de forma completa, permite conexões de dentro para fora da rede sem nenhuma configuração explícita para cada tipo de sistema interno. “O ASA esta sempre em execução, monitorando os pacotes para garantir que eles sejão válidos” (Cisco Systems, 2003, p. 1-3, tradução nossa).

ASA aplica-se aos slots tradução dinâmica e slots tradução estática. “Você cria slots de tradução estática com o comando estático e slots de tradução dinâmica com o comando global. Coletivamente, os dois tipos de slots de tradução são referidos como *xlates*” (Cisco Systems, 2003, p. 1-3, tradução nossa).

O ASA segue algumas regras:

> • Nenhum pacote pode atravessar o firewall PIX sem uma conexão e estado.
> • O Tráfego do PIX Firewall não pode sair pela mesma interface de rede que entrou.
> • Conexões de saída ou estados são permitidos, exceto os expressamente negados por listas de controle de acesso. [...]
> • Conexões de entrada ou estados são negados, exceto os expressamente permitidos.
> • Todos os pacotes ICMP são negados a menos que especificamente permitido.
> • Todas as tentativas de contornar as regras anteriores são descartadas e uma mensagem é enviada ao *syslog*.
> (Cisco Systems, 2003, p. 1-3, tradução nossa).

A Cisco Systems (2003) afirma que o PIX Firewall lida com transferências de dados UDP da mesma maneira que lida com o tráfego TCP.

> Tratamento especial permite que DNS, Archie, StreamWorks, H.323, e RealAudio trabalhem de forma segura. A PIX Firewall cria informações de estado de uma conexão UDP quando um pacote UDP é enviado a partir da rede interna. Pacotes de resposta resultante desse tráfego são aceitos se corresponderem às informações de estado de conexão. As informações de estado de conexão são excluídas após um curto período de inatividade. (Cisco Systems, 2003, p. 1-4, tradução nossa).

A Cisco Systems (2003) explica que quando um pacote de saída chega a uma interface de nível mais elevado de segurança, o PIX Firewall verifica se o

pacote é válido baseado no ASA, e então define se os pacotes devem ser entregues ao destino ou não.

> Caso não, então o pacote é direcionado a uma nova conexão, e o PIX Firewall cria um slot de tradução na sua tabela de estado para conexões. A informação que o PIX Firewall armazena no slot de tradução inclui o endereço IP e um endereço IP exclusivo atribuído pelo Network Address Translation (NAT), Port Address Translation (PAT), ou Identidade (que usa o endereço interno como o endereço externo). O PIX Firewall, então muda o endereçamento IP do pacote de origem para o endereço exclusivo global, modifica a soma de verificação e outros campos conforme necessário, e encaminha o pacote para a interface com menor nível de segurança. (Cisco Systems, 2003, p. 1-4, tradução nossa).

Quando um pacote de entrada chega a uma interface externa como a interface de saida, ele primeiro passa pelos critérios Adaptive Security do PIX Firewall. “Se o pacote passar nos testes de segurança, a PIX Firewall remove o endereço IP de destino, bem como o endereço IP interno que é inserido em seu lugar. O pacote é então encaminhado para a interface protegida” (Cisco Systems, 2003, p. 1-4, tradução nossa).

É importante frizar que o tráfego do PIX Firewall nunca pode sair pela mesma interface pela qual entrou.

No PIX Firewall “o recurso Network Address Translation (NAT) funciona substituindo, ou traduzindo, endereços de *hosts* em uma interface para um "endereço global" associada à outra interface” (Cisco Systems, 2003, p. 1-5, tradução nossa). Esta funcionalidade pode ser observada no Anexo C.

A Cisco Systems (2003) alega que para ajudar a simplificar o roteamento da rede, o recurso NAT, a partir da versão 6.2 do PIX Firewall, também traduz endereços esternos, controlando os endereços que podem aparecer na rede interna.

Se for necessário proteger o acesso aos endereços apenas de outras redes dentro da mesma organização, pode-se usar qualquer conjunto de endereços privados para o pool de endereços de tradução.

> Por exemplo, se você quiser proteger os endereços hospedeiros na rede do Departamento de Finanças (conectado à interface dentro do PIX Firewall) da exposição ao conectar ao Departamento de Vendas da rede (ligada à interface do perímetro do firewall PIX), você pode configurar tradução usando qualquer conjunto de endereços disponíveis na rede de vendas. O efeito é que os hosts da rede Finanças aparecem como endereços locais na rede de vendas. (Cisco Systems, 2003, p. 1-5, tradução nossa).

Já se os endereços que necessitam ser protegidos requerem acesso à Internet, deve-se usar apenas endereços oficiais da Internet registrados no Network Information Center (NIC) para o pool de endereços de tradução.

> Por exemplo, se você quiser proteger endereços de *hosts* na rede de vendas (conectado a uma interface de perímetro do PIX Firewall) de exposição ao fazer conexões com a Internet (acessível através da interface externa do PIX Firewall), você pode configurar tradução usando um pool de endereços registrados na interface externa. O efeito é que os *hosts* da Internet enxergam apenas os endereços da Internet para a rede de vendas e não os endereços na interface de perímetro. (Cisco Systems, 2003, p. 1-5, tradução nossa).

Segundo a Cisco Systems (2003), ao considerar NAT, também é importante considerar se existe um número igual de endereços para *hosts* internos, senão, alguns *hosts* internos podem não ter acesso de rede ao fazer uma conexão. A Cisco recomenda neste caso, que sejam solicitados endereços adicionais ao NIC ou usar Port Address Translation (PAT). “PAT usa um único endereço externo para gerenciar até 64 mil conexões simultâneas. Para sistemas internos, NAT traduz o endereço IP de origem dos pacotes de saída (definido na RFC 1631). Ele suporta tradução dinâmica e estática” (Cisco Systems, 2003, p. 1-5, tradução nossa).

> NAT permite que endereços privados (definido no RFC 1918) possam ser atribuídos aos sistemas internos, ou manter existentes endereços inválidos. NAT também oferece segurança adicional, ocultando a identidade verdadeira da rede de sistemas internos para a rede externa. (Cisco Systems, 2003, p. 1-5, tradução nossa).

A Cisco Systems (2003) afirama que PAT utiliza a porta de remapeamento, permitindo que um único endereço IP válido suporte tradução de endereços IP para até 64 mil objetos *xlate* ativos. Além disso, “PAT minimiza o número de endereços IP globais válidos necessárias para apoio privado ou esquemas de endereçamento interno inválido” (Cisco Systems, 2003, p. 1-5, tradução nossa).

O Anexo D demonstra como PIX Firewall utiliza o recurso PAT.

> PAT não funciona com aplicativos multimídia que têm um fluxo de dados de entrada diferente do caminho de controle de saída. PAT oferece segurança adicional, ocultando a identidade verdadeira da rede de sistemas internos para rede externa. (Cisco Systems, 2003, p. 1-5, tradução nossa).

Outra classe de tradução de endereços no PIX Firewall é a tradução estática. “Tradução estática permite substituir um endereço externo de IP fixo para

um endereço interno. Isto é útil para servidores que requerem endereços IP fixos para acesso a partir da Internet" (Cisco Systems, 2003, p. 1-5, tradução nossa).

Segundo a Cisco Systems (2003), o PIX Firewall tem como característica o recurso de Identidade que permitir que a tradução de endereços possa ser desativada.

> Se os sistemas internos têm endereços globais únicos e válidos, o recurso de Identidade permite que NAT e PAT possam ser seletivamente desativados para esses sistemas. Esta característica torna os endereços da rede interna visível para a rede externa. (Cisco Systems, 2003, p. 1-5, tradução nossa).

A Cisco Systems (2003) define Cut-Through Proxy como outra característica do PIX Firewall, o qual é um recurso exclusivo que permite autenticação baseada no usuário de conexões de entrada ou de saída.

> Um servidor *proxy* analisa todos os pacotes na camada sete do modelo OSI, que é uma função de tempo de processamento intenso. Por outro lado, a PIX Firewall usa *cut-through proxy* para autenticar uma conexão e então permitir que o tráfego flua de forma rápida e direta. (Cisco Systems, 2003, p. 1-6, tradução nossa).

Segundo a Cisco Systems (2003), Cut-Through Proxy permite um nível muito mais refinado de controle administrativo baseado nas verificações de endereços IP de origem das conexões. "Ele permite que políticas de segurança possam ser executadas com base em contas de usuários individuais" (Cisco Systems, 2003, p. 1-6, tradução nossa).

> Conexões podem ser autenticadas com um ID de usuário e senha antes de serem estabelecidas, e de mesmo modo, as senhas dinâmicas ou *tokens* de segurança são suportadas para uma maior segurança. Autenticação e autorização são suportadas por HTTP, Telnet, ou conexões FTP. (Cisco Systems, 2003, p. 1-6, tradução nossa).

PIX Firewall possui também suporte a protocolos de roteamento. A Cisco Systems (2003) notifica que PIX Firewall em sua versão 6.3, já introduz o suporte para o Open Shortest Path First (OSPF), que permite PIX Firewall a participar plenamente na dinâmica atualizações de roteamento dedicada com dispositivos de roteamento.

> PIX Firewall antes da versão 6.3 suportava apenas Routing Information Protocol (RIP) Versão 2.

> Ao usar RIP, PIX Firewall só escutava em modo passivo e/ou transmissões de uma rota padrão. O PIX Firewall suporta padrões Cisco IOS software, os quais obedecem as RFC 1058, RFC 1388, e RFC 2082 para RIPv2 com texto e chave MD5 de autenticação. A PIX Firewall suporta uma chave e ID da chave por interface. (Cisco Systems, 2003, p. 1-6, tradução nossa).

Segundo a Cisco Systems (2003), PIX Firewall fornece também integração com serviços de autenticação, autorização e contabilidade (AAA – do inglês *authentication*, *authorization*, *and accounting*). “PIX Firewall permite que você defina grupos separados de TACACS + ou servidores RADIUS para especificar diferentes tipos de tráfego.” (Cisco Systems, 2003, p. 1-6, tradução nossa).

A Cisco Systems (2003) alega ainda que desde a ersão 5.3, o PIX Firewall utiliza listas de acesso para controlar as conexões entre redes internas e externas.

> PIX Firewall versão 6.3 melhora a sua capacidade de registrar informações sobre as atividades associadas com listas de acesso específicas de controle (ACLs). Na versão 6.3 também é possível que você adicione comentários a cada ACL, para que você possa descrever a finalidade e efeito esperado de cada entrada. (Cisco Systems, 2003, p. 1-7, tradução nossa).

É possível usar listas de acesso para controlar as conexões com base nos endereços de origem, nos endereços de destino, ou nos protocolos. A Cisco Systems (2003) recomenda fazer listas de acesso mais restritivas, especificando o endereço de origem remoto, o endereço de destino local, e o protocolo.

“Um recurso chamado TurboACL foi introduzido no PIX Firewall Versão 6.2, que melhora a maneira com que o PIX Firewall controla os processos de listas com grande acesso” (Cisco Systems, 2003, p. 1-7, tradução nossa).

Segundo a Cisco Systems (2003), o método pelo qual as pesquisas do PIX Firewall buscam uma entrada na lista de acesso foram melhorados para reduzir o tempo gasto na procura de listas de acesso com grande porte. “TurboACL suporta listas de acesso com até 16 mil entradas” (Cisco Systems, 2003, p. 1-7, tradução nossa).

A Cisco Systems (2003) confirma que quando usado com um servidor AAA, PIX Firewall permite que sejam criadas listas de acesso para conexões de controle para cada usuário.

> A partir da Versão 6.2 do PIX Firewall, a lista de acesso exigida por usuário é baixada do servidor AAA baseada no perfil do usuário. Nenhuma configuração adicional na lista de acesso é exigida em qualquer Firewall PIX. Esta nova funcionalidade reduz a complexidade e melhora a

> escalabilidade das listas de acesso por usuário. (Cisco Systems, 2003, p. 1-7, tradução nossa).

A Cisco Systems (2003) expõe a introduação de agrupamento de objetos em PIX Firewall em sua versão 6.2, o qual reduz a complexidade de configuração e melhora a escalabilidade para redes grandes ou complexas. “Agrupamento de objetos permite aplicar regras de acesso para grupos lógicos de objetos de rede” (Cisco Systems, 2003, p. 1-8, tradução nossa).

> Quando você aplica um comando PIX Firewall para um grupo de objeto, o comando afeta todos os objetos de rede definidos dentro do grupo. Isso pode reduzir um número muito grande de regras de acesso a um número gerenciável, que reduz o tempo gasto para configurar e solucionar problemas com regras de acesso em redes grandes ou complexos. (Cisco Systems, 2003, p. 1-8, tradução nossa).

Redes virtuais de área local (VLANs) são usadas para criar domínios de difusão separados em uma única rede comutada. “PIX Firewall versão 6.3 pode rotear o tráfego entre esses domínios de transmissão, ao aplicar a política de firewall para a sua rede” (Cisco Systems, 2003, p. 1-8, tradução nossa).

> PIX Firewall agora suporta 802.1Q, o qual permite que o tráfego de várias VLANs possa ser trocado por via de um único link físico. Com a versão 6.3, você pode definir várias interfaces lógicas para uma única interface física, e atribuir VLANs diferentes para cada interface lógica. (Cisco Systems, 2003, p. 1-8, tradução nossa).

Segundo a Cisco Systems (2003), PIX Firewall também possui recurso de encaminhamento Unicast Reverse Path (Unicast RPF), também conhecida como "pesquisa de rota inversa," o qual fornece filtragem de entrada e saída para ajudar a evitar a falsificação de IP.

> Este recurso verifica os pacotes de entrada para a integridade do endereço IP de origem, e verifica se os pacotes destinados a hosts fora do domínio gerenciado tem fonte de endereços IP verificáveis por vias nas entidades de aplicação da tabela de roteamento local. (Cisco Systems, 2003, p. 1-9, tradução nossa).

A Cisco Systems (2003) profere que PIX Firewall possui ainda o recurso Mail Guard, o qual oferece acesso seguro para conexões Simple Mail Transfer Protocol (SMTP) de fora para dentro de um servidor de mensagens.

> Este recurso permite que um servidor de correio único possa ser implantado dentro da rede interna sem que seja exposto a problemas de segurança conhecidos com algumas implementações do servidor SMTP. Isso elimina a necessidade de um relé de e-mail externo (ou *bastion host*) do sistema. (Cisco Systems, 2003, p. 1-9, tradução nossa).

Outro recurso implementado em PIX Firewall é o Flood Guard, o qual a Cisco Systems (2003) explica como sendo uma solução para controlar a tolerância ao serviço AAA com tentativas de login sem resposta. “Isso ajuda a impedir um ataque de negação de serviço (DoS) particularmente em serviços de AAA. Este recurso otimiza o uso do sistema AAA. Ele é ativado por padrão” (Cisco Systems, 2003, p. 1-9, tradução nossa).

PIX Firewall também possui correção de DNS, a qual identifica cada DNS de saída ao resolver a solicitação, e só permite uma resposta de DNS único.

> O hospedeiro pode consultar vários servidores de uma resposta (no caso em que o primeiro servidor demore a responder), mas apenas a primeira resposta ao pedido é permitida. Todas as respostas adicionais para o pedido são ignoradas pelo firewall. A correção DNS é configurável e ativada por padrão. (Cisco Systems, 2003, p. 1-9, tradução nossa).

Segundo a Cisco Systems (2003), PIX Firewall, para manter a segurança da rede, também possui recursos para bloquear conteúdos ActiveX e filtrar aplicações Java.

A Cisco Systems (2003) recomenda, para reduzir a tarefa administrativa e melhorar a eficácia de filtragens, usar o PIX Firewall em conjunto com um servidor separado que execute filtragem de URL, pois o PIX Firewall verifica pedidos de URL de saída com a política definida no servidor de filtragem de URL.

O recurso Configurable Proxy Pinging permite que PIX Firewall controle o acesso a interfaces ICMP. “Este recurso protege PIX Firewall da detecção de interfaces de usuários em uma rede externa” (Cisco Systems, 2003, p. 1-10, tradução nossa).

Segundo a Cisco Systems (2003), PIX Firewall também possui suporte a protocolos e aplicações específicas como: Aplicação de Fiscalização de Obra; Voz sobre IP; Aplicações Multimidia; LDAP V2 e ILS; NetBIOS sobre IP; Encaminhamento de Transmissões Multicast; e Rede Privada Virtual (VPN).

A Cisco Systems (2003) também expõe que é possível usar PIX Firewall em um ambiente de trabalho pequeno.

Do mesmo modo que qualquar *firewall*, o PIX Firewall pode ser acessado e monitorado de várias formas.

> PIX Firewall versão 6.3 permite uma conexão de gerenciamento remoto com a interface interna de um PIX Firewall ao longo de um túnel VPN. Esse recurso é projetado para permitir que um administrador possa gerenciar remotamente um PIX Firewall usando como um dispositivo Easy VPN Remote, que normalmente tem um endereço IP dinamicamente atribuído à sua interface externa. (Cisco Systems, 2003, p. 1-21, tradução nossa).

A Cisco Systems (2003) indica como mecanismo de gerenciamento do PIX Firewall o Cisco PIX Device Manager (PDM), o qual é uma ferramenta de configuração baseada em navegação que permite instalar, configurar e monitorar o PIX Firewall a partir de uma interface gráfica de usuário (GUI), sem qualquer conhecimento amplo da interface PIX Firewall de linha de comando (CLI). O Anexo E mostra como os usuários são autenticados para acessar a interface gráfica de gerênciamento do PIX Firewall.

> PIX Firewall versão 6.2 ou superiores fornecem um método mais flexível de autenticação e autorização de acesso administrativo ao PIX Firewall. Semelhante ao software Cisco IOS de autorização de comando, PIX Firewall agora suporta até 16 níveis de privilégios a serem atribuídos aos comandos CLI. Você pode criar contas de usuário ou contextos de *login* ligados a esses níveis de privilégios seja localmente ou usando um servidor TACACS +. (Cisco Systems, 2003, p. 1-9, tradução nossa).

Telnet também pode ser usado para gerenciamento do PIX Firewall. Segundo a Cisco Systems (2003), a interface Telnet permite gerenciar remotamente o PIX Firewall através da interface de console, entretanto esse acesso é protegido por uma senha e limitado apenas a interface interna da rede.

Entretanto, a Cisco Systems (2003) afirma que é possível utilisar funcionalidades SSH para configurar e moniturar remotamente o PIX Firewall fornecendo capacidades de encriptação e autenticação.

A Cisco Systems (2003) assegura que PIX Firewall Possui ainda muitas outras funcionalidades, tanto para gerenciamento quanto para monitoramento de recursos e políticas de segurança, tais como: NTP, atualizações automáticas, captura de pacotes, SNMP, XDMCP, Syslog, Registros de URL e FTP, além de ser interoperável com o Sistema de Detecção de Intrusão Cisco (Cisco IDS).

CONCLUSÃO

Com o presente trabalho é possível concluir que uma política de segurança aplicada a um *firewall* não é apenas a programação do bloqueio de portas e serviços, mas sim um conjunto de regras e recursos que devem ser cuidadosamente ativados para manter uma rede com segurança sem desperdiçar desempenho e garantindo a integridade das informações.

Para estabelecer as políticas de segurança em um *firewall*, é necessário analisar quais os tipos de informação que trafegam pela rede, e preferencialmente bloquear tudo o que não for apropriado para o tráfego da mesma, assim não estarão sendo desperdiçados recursos que devem ser utilizados para o propósito da organização.

Pode-se concluir também que o PIX Firewall, alvo do trabalho apresentado, é uma solução bastante completa, que possui um número elevado de recursos e funções, os quais têm como objetivo principal fornecer segurança para a rede sem limitar os serviços que ela pode oferecer.

Atuando desde a camada de rede até a camada de aplicação, PIX Firewall é uma solução que pode ser utilizada em qualquer tipo de rede, desde que a mesma trabalhe sobre a pilha do Protocolo TCP/IP.

Compreende-se que PIX Firewall é uma ferramenta de propriedade da Cisco Systems, a qual fornece qualquer tipo de informação referente ao produto. Entretanto, PIX Firewall não é uma solução gratuita, o que se torna um de seus únicos problemas diante de outras soluções livres, ele também só opera a partir de um hardware específico (salvo em casos de virtualização), o que limita a sua utilização, mas ao mesmo tempo, eleva seu desempenho e confiabilidade.

PIX Firewall não é difícil de ser configurado e gerenciado, mesmo porque, possui uma interface gráfica voltada para navegadores que propõe a administração de suas funções sem a necessidade de acessar o modo *shell* do sistema, outrossim, para quem já trabalha ou trabalhou com as soluções da Cisco Systems, não encontrará dificuldades em opera-lo em seu modo texto.

Por fim, podemos observar que PIX Firewall é uma solução para redes que dependem de segurança, e que não possuem tempo para disperdiçar em implantações de diversos *firewalls* sem ter garantia de serviço, pois PIX Firewall já possui diversos recursos de segurança habilitados por padrão e além de ser uma

ferramenta que garante a proteção da rede sem perder desempenho e funcionalidades, possui suporte completo fornecido pela Cisco Systems.

REFERÊNCIAS

CISCO SYSTEMS INC. **Cisco PIX Firewall and VPN Configuration Guide.** California, 2003. v. 6.3.

CISCO SYSTEMS INC. **Cisco PIX Firewall Command Reference.** California, 2004. v. 6.3.

CISCO SYSTEMS INC. **Cisco Secure PIX FireWall Advanced**: Student Guide. California, 2000. v. 1.01.

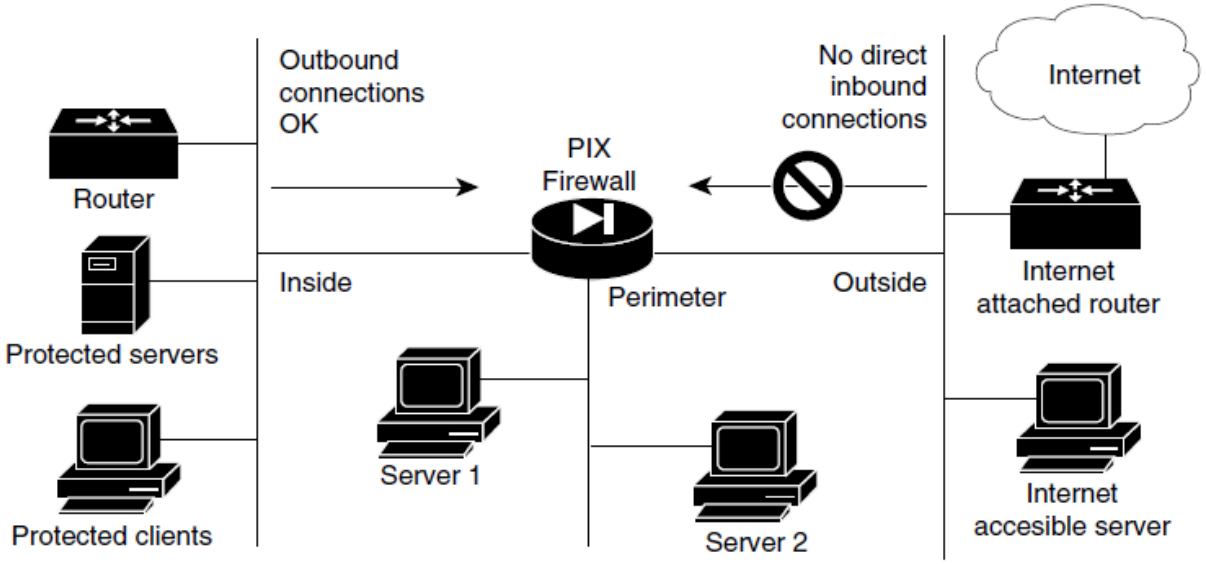
CISCO SYSTEMS INC. **Cisco Security Appliance Command Line Configuration Guide.** California, 2008. v. 7.2.

FREIRE, Alexandre. **Sistemas de Firewall e Defesa de Perímetros**. Portal Módulo Security, 2004. Disponível em: <http://www.magicweb.com.br/afreire/publicacoes.htm>. Acesso em: 09 Out. 2011.

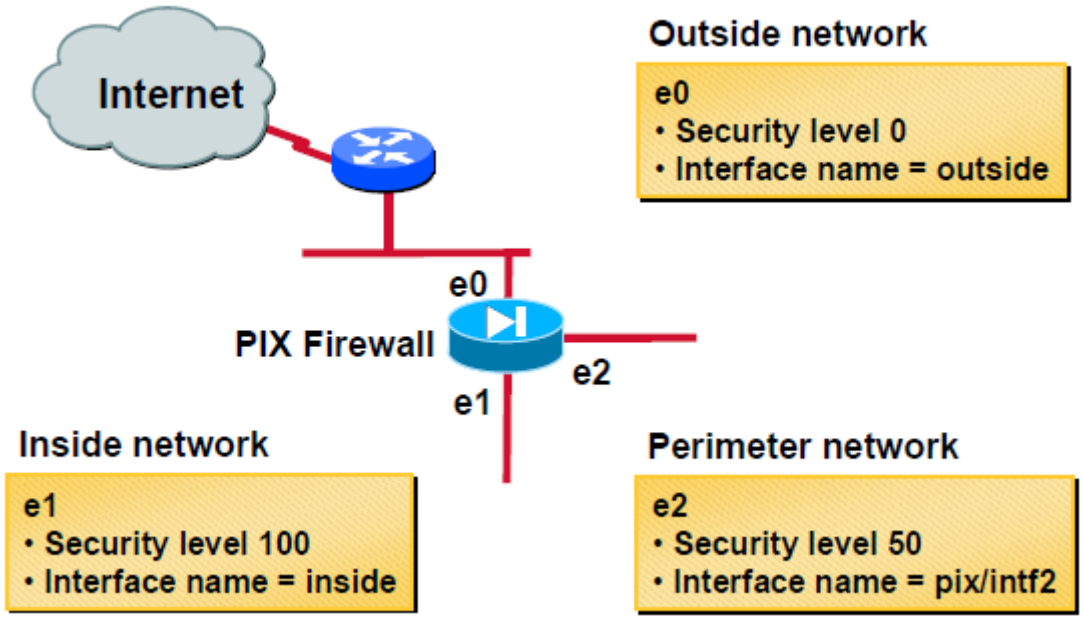
NETO, Urubatan. **Dominando Linux Firewall Iptables**. Rio de Janeiro: Ciência Moderna, 2004.

ANEXOS

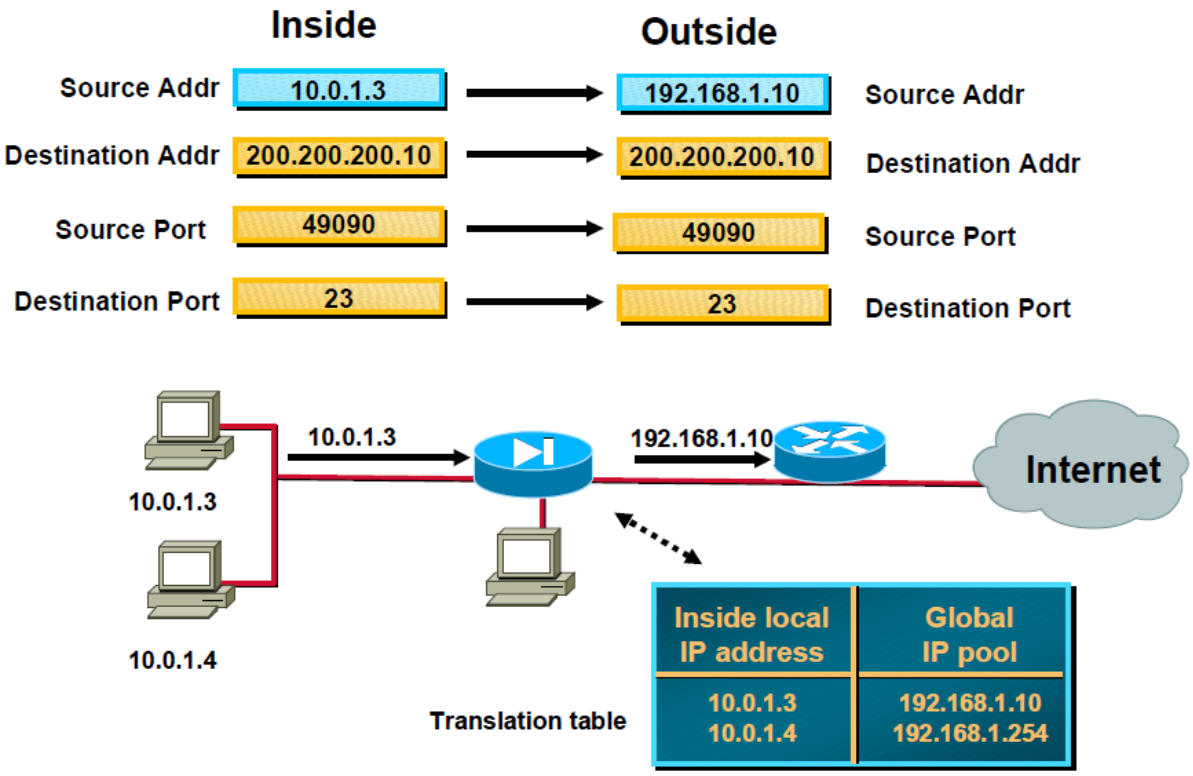
ANEXO A – O PIX Firewall em uma rede



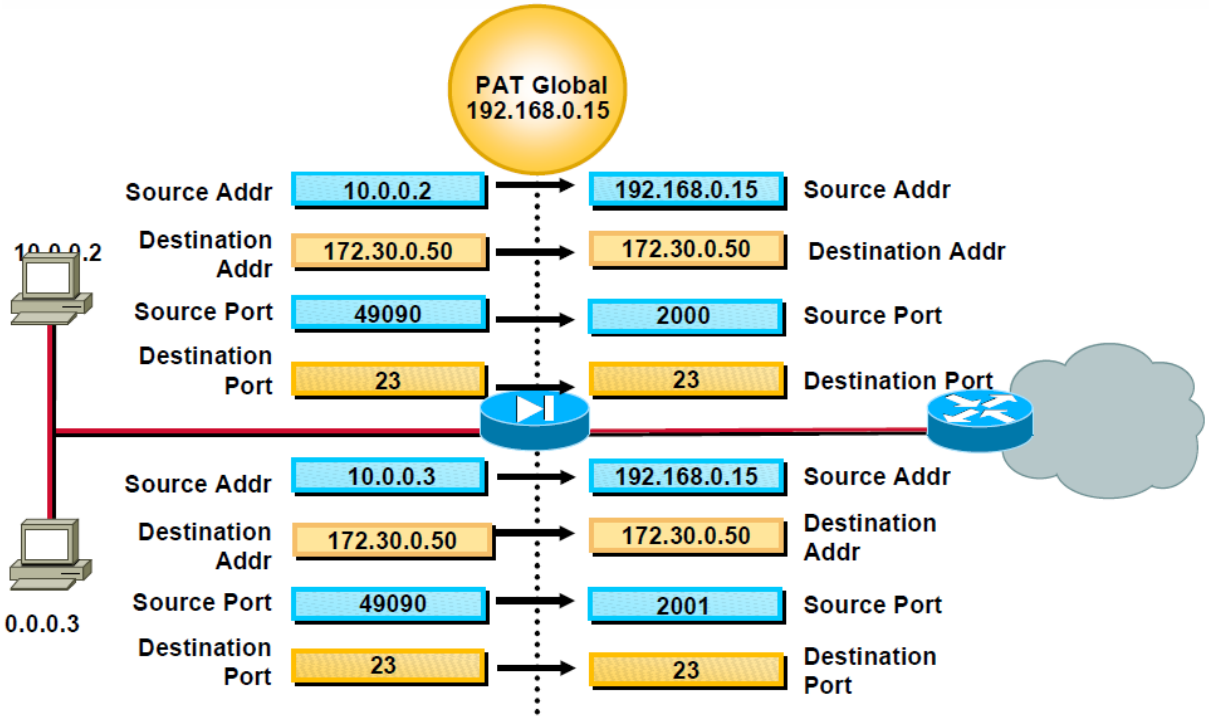
ANEXO B – Níveis de segurança do ASA



ANEXO C – PIX Firewall Executando a Conversão de Endereços com NAT



ANEXO D – PIX Firewall Executando a Tradução de Endereços de Porta com PAT



ANEXO E – Página de Autenticação Segura