



**Proposta de Hardening em Conformidade com a ISO 27001
para um Firewall em Linux com Balanceamento de Carga**

Dorival Moreira Machado Junior

Lavras
Minas Gerais - Brasil
2008

Dorival Moreira Machado Junior

**Proposta de Hardening em Conformidade com a ISO 27001
para um Firewall em Linux com Balanceamento de Carga**

Monografia de Pós-Graduação “*Lato Sensu*”
apresentada ao Departamento de Ciência da
Computação da Universidade Federal de Lavras,
para obtenção do título de Especialista em
“Administração em Redes Linux”.

Orientador
Prof. Msc. Sandro Melo

Lavras
Minas Gerais - Brasil
2008

Dorival Moreira Machado Junior

**Proposta de Hardening em Conformidade com a ISO 27001
para um Firewall em Linux com Balanceamento de Carga**

Monografia de Pós-Graduação “*Lato Sensu*”
apresentada ao Departamento de Ciência da
Computação da Universidade Federal de Lavras,
para obtenção do título de Especialista em
“Administração em Redes Linux”.

Aprovada em 28 de setembro de 2008.

Profa. Dra. Marluce Rodrigues Pereira

Prof. Esp. Samuel Pereira Dias

Prof. Msc. Sandro Melo
(orientador)

LAVRAS
MINAS GERAIS – BRASIL

Dedico esta monografia à toda
minha família, em especial aos meus
pais, Dorival e Divina, à minha
amada esposa Márcia e ao meu filho
Giovanni.

Agradecimentos:

Agradeço a Deus que me proveu esta oportunidade de aprendizado, bem como a inteligência necessária para adquirir tal conhecimento.

Agradeço aos melhores pais do mundo, Dorival e Divina, pelo carinho, incentivo e apoio contínuo aos estudos.

Agradeço à minha esposa Márcia pela paciência e compreensão perante minha ausência e noites reduzidas de sono durante o período de curso, bem como pelo seu amor e companheirismo.

Agradeço ao meu filho Giovanni pelos choros e pedido de atenção exclusiva enquanto eu desenvolvía este trabalho, mas sobretudo pela alegria que ele me proporciona.

Agradeço aos meus irmãos Julio Cesar e Julio Henrique pela presença familiar.

Agradeço aos professores da UFLA que transmitiram grande conhecimentos na área estudada.

Agradeço ao professor Sandro, que me conduziu no desenvolvimento desta monografia, transmitindo seus conhecimentos em larga escala.

Agradeço aos novos amigos que surgiram devido a existência deste curso.

Agradeço à Faculdade Libertas e a Contabilidade Dorival Machado, instituições que abriram as portas para a aplicação prática desta monografia.

Sumário

1 Introdução	1
1.1 Objetivo	2
1.2 Motivação	2
1.3 Estado da arte	3
1.4. Metodologia	4
1.4. Estrutura dos capítulo	5
2 Fundamentação teórica sobre tecnologia de <i>Firewall</i>	7
2.1 Firewall	7
2.2 Firewall para a camada sete	8
2.3 Balanceamento de carga	9
2.4 Iptables	11
2.5 Iproute	12
3 Proposta de <i>hardening</i> para um sistema <i>firewall</i> baseado em Debian	14
3.1 Sobre a NBR ISO/IEC 27001	14
3.2 O processo de <i>hardening</i>	17
3.3 Disposição regular das etapas do <i>hardening</i>	18
3.3.1 Controles da ISO 27001 inerentes à política de segurança	19
3.3.2 Controles da ISO 27001 inerentes à organização da segurança da informação	21

3.3.3 Controles da ISO 27001 inerentes à gestão de ativos	21
3.3.4 Controles da ISO 27001 inerentes à segurança física	21
3.3.5 Controles da ISO 27001 inerentes ao gerenciamento das operações e comunicações	22
3.3.6 Controles da ISO 27001 inerentes a proteção contra códigos maliciosos	22
3.3.7 Controles da ISO 27001 inerentes a cópias de segurança	24
3.3.8 Controles da ISO 27001 inerentes a manuseio de mídias	25
3.3.9 Controles da ISO 27001 inerentes a monitoramento	25
3.3.10 Controles da ISO 27001 inerentes ao gerenciamento de acesso de usuário	27
3.3.11 Controles da ISO 27001 inerentes a responsabilidade dos usuários	27
3.3.12 Controles da ISO 27001 inerentes ao controle de acesso ao sistema operacional	28
3.3.13 Controles da ISO 27001 inerentes a computação móvel e trabalho e remoto	31
3.3.14 Controles da ISO 27001 inerentes a aquisição, desenvolvimento e manutenção de sistemas de informação	31
3.3.15 Controles da ISO 27001 inerentes a segurança dos arquivos do sistema	32
3.3.16 Controles da ISO 27001 inerentes a gestão de incidentes de segurança da informação	33
3.3.17 Controles da ISO 27001 inerentes a gestão de continuidade do negócio	34
3.3.18 Controles da ISO 27001 inerentes a conformidade	34
3.3.19 Controles da ISO 27001 inerentes a auditoria de sistemas de informação	35

4 Firewall	37
4.1 Regras básicas para roteamentos	37
4.2 Recursos de PAT	38
4.3 Recursos de bloqueio para rede externa	38
4.4 Recursos de excessão às regras	39
4.5 Implementação da camada sete	39
4.6 Liberação de portas para repasse	40
4.7 Definição de ping	40
4.8 Proteção contra formas de ataque comum	41
4.9 Definição de portas utilizadas	41
4.10 Recursos de NAT	41
4.11 Segregação de rede	42
4.12 Demais regras inerentes à realidade da empresa	43
5 Balanceamento de carga	45
5.1 Detecção das conexões e regras existentes	45
5.2 Balanceamento entre as conexões de internet	46
5.2.1 Arquivo rt_tables	46
5.2.2 Rotas nas tabelas auxiliares	46
5.2.3 Rotas na tabela principal	48
5.2.4 Regras de roteamento	48
5.2.5 Verificação continuada do balanceamento	49

6 Resultados obtidos	51
6.1 Resultados obtidos no caso A	52
6.2 Resultados obtidos no caso B	52
7 Conclusão	54
7.1 Propostas de trabalhos futuros	54
8 Referências Bibliográficas	55
9 Apêndices	58
10 Anexos	81

Lista de Figuras

Figura 1 – firewall	7
Figura 2 – ambiente com firewall recebendo dois <i>link</i> externos	9
Figura 3 – arquivo <code>/etc/iproute2/rt_tables</code>	12
Figura 4 – linha cronológica do padrão ISO 27000	15
Figura 5 – modelo PDCA de acordo com (ISO 27001,2006)	17
Figura 6 – trecho do arquivo <code>/etc/fstab</code>	22
Figura 7 – trecho de monitoramento registrado pelo <code>Snoopy Logger</code>	25
Figura 8 - linhas inseridas no <code>squid.conf</code> para geração do LOG personalizado	25
Figura 9 - trecho de LOG personalizado gerado pelo <code>Squid</code>	25
Figura 10 - trecho do arquivo <code>/etc/pam.d/su</code>	27
Figura 11 - trecho do arquivo <code>/etc/pam.d/login</code>	27
Figura 12 - trecho do arquivo <code>/etc/pam.d/time.conf</code>	27
Figura 13 - trecho do <code>/etc/passwd</code> onde apenas root e usuário estratégico possuem um shell válido	28
Figura 14 - trecho do arquivo <code>/etc/adduser.conf</code> definindo um caminho invalido de <i>shell</i> para novos usuários	28
Figura 15 - trecho do arquivo <code>/etc/inittab</code> referente a desabilitação do CTRL+ALT+DEL	28
Figura 16 - trecho do arquivo <code>/etc/ssh/sshd_config</code> referente a desabilitação de <i>login</i> remoto do root e alteração da porta ssh	28
Figura 17 - arquivo <code>/etc/apt/sources.list</code> com repositórios oficiais Debian ..	31
Figura 18 - política restritiva no <code>Iptables</code>	36
Figura 19 - utilização comparativa de SNAT e MASQUERADE	41
Figura 20 - modelo de segregação de rede em ambiente com muitos serviços ou usuários	43
Figura 21 - arquivo <code>rt_tables</code> recriado com duas tabelas auxiliares	46
Figura 22 - saída do comando <code>ip show table velox</code> e descrição de resultado ..	46
Figura 23 - saída do comando <code>ip route show table main</code>	47
Figura 24 - saída do comando <code>ip rule</code>	48
Figura 25 - agendamento do Apêndice D através do <code>cron</code>	49
Figura 26 – trecho do <code>/var/log/message</code> com resultados de execução do Apêndice D	49

Lista de Tabelas

Tabela 1 - ações realizadas pelo <code>iptables</code>	11
Tabela 2 - objetos de configuração do comando <code>ip</code>	12
Tabela 3 - comparação e descrição de conteúdos das normas ISO e BS.	15
Tabela 4 - descrição das etapas do modelo PDCA da ISO 27001.	17
Tabela 5 - proposta de ordem lógica para realização das etapas do hardening	19
Tabela 6 - procedimentos para controle de reforço no acesso ao sistema operacional	29

Lista de Abreviações e Siglas

ABNT – Associação Brasileira de Normas Técnicas

BS – *British Standard*

CB-21 – Comitê Brasileiro de Computadores e Processamento de Dados

CBQ – *Class Based Queueing*

HTTP – *Hipertext Transfer Protocol*

HTTPS - *HyperText Transfer Protocol Secure*

IEC - *International Electrotechnical Commission*

IP – *Internet Protocol*

ISO - *International Organization for Standardization*

NAT – *Network Address Translation*

NBR – *Norma brasileira*

OSI – *Open Systems Interconnection*

PAT – *Port Address Translation*

SARG - *Squid Analisys Report Generator*

TCP – *Transmission Control Protocol*

Resumo

Esta monografia apresenta os requisitos bem como as sugestões de implementação para possibilitar ao computador destinado à função de *firewall*, uma adequação à norma ABNT NBR ISO/IEC 27001, garantindo assim uma melhoria significativa no quesito segurança da informação. É apresentado uma implementação de modelo de regras de *firewall* em conformidade com a mesma norma, utilizando-se de *script* afim de automatizar o processo. Por fim são apresentados os recursos necessários para implementação de um balanceamento de carga com dois *link* externos, assim como a sugestão de implementação prática.

Palavras-chave: ISO 27001, hardening, firewall, balanceamento de carga, debian.

Capítulo 1

Introdução

A informação sempre foi inerente ao ser humano, ou seja, desde o seu nascimento ele tende a absorver todas as informações possíveis ao seu redor. Durante sua vida, passando por escolas, cursos ou a própria convivência em seu grupo, ele adquire conhecimentos mesmo que involuntariamente.

Na atualidade, o interesse pelo fator informação passou a ter um aumento exponencial. O principal motivo que levou a esse aumento, é a conscientização do ser humano de que informação é poder, ou seja, através da informação, pode-se levar uma instituição ao sucesso ou fracasso. Esta atualidade, também pode ser conhecida como “sociedade da informação”, ou seja, um ambiente com grande excesso de informações disponíveis, juntamente com a necessidade do ser humano em adquirí-las.

Devido ao avanço das tecnologias de comunicação, o ambiente de negócios mundial é cada vez mais interconectado. Em contrapartida, as ameaças virtuais e reais também avançam, possibilitando o roubo ou extravio de informações, seja partindo de um ataque externo ou interno a uma organização. O fato é que possivelmente as informações da organização, sendo então um dos principais ativos, estarão vulneráveis.

1.1. Objetivo

Esta monografia tem por objetivo apresentar uma proposta de ajuste fino em uma máquina *firewall*, buscando uma conformidade com a norma ABNT NBR ISO/IEC 27001. Inclui-se neste ajuste, uma proposta de implementação das regras de *firewall* bem como um balanceamento de carga entre duas conexões externas.

1.2. Motivação

No ambiente empresarial, o acesso irrestrito a internet, com livre navegação, ferramentas ponto-a-ponto e mensageiros instantâneos, geram problemas de consumo de banda, além de estar utilizando os equipamentos para outras finalidades não condizentes com os interesses da empresa.

Esta conduta permite a possibilidade de brechas na segurança do ambiente, e conseqüentemente o comprometimento das informações importantes então armazenadas. Assim, é motivado um refinamento da segurança da máquina que é porta de entrada para a rede interna, bem como a implementação segura das regras de controle de tráfego.

A instabilidade de sinais de internet via rádio, ou a possibilidade de falha técnica em outros meios de transmissão como cabeamento, faz com que empresas utilizem uma segunda conexão como forma de contingência, afim de garantir a produtividade contínua do negócio. Esse fator motiva a implementação de um balanceamento de carga, utilizando ambas as conexões de forma simultânea.

1.3. Estado da arte

O serviço de *firewall* e balanceamento de carga pode ser feito atualmente através de várias distribuições Linux, como as primárias: Debian, Red Hat e Slackware, bem como as secundárias ou *fork*: CentOS, Coyote Linux, Ubuntu, OpenSUSE, Fedora, entre outras. Todas estas utilizando ferramentas idênticas ou similares as quais são sugeridas nesta monografia.

O Debian foi a distribuição escolhida para esta monografia primeiramente pelo fato de possuir um maior *know how*, diante das demais distribuições. Porém outros fatores também foram levados em consideração, como por exemplo a presença no ambiente empresarial.

Esta distribuição se mantém estável, com lançamento frequente de pacotes de atualização (DEBIAN, 2008), mantendo o sistema sempre atualizado no quesito segurança. Em seu todo, o Debian é uma distribuição robusta, porém como todo bom sistema, requer um procedimento de refinamento e ajuste da segurança, uma vez que as técnicas de invasão são cada vez mais diversificadas. Este refinamento, também conhecido tecnicamente como *hardening*, é proposto observando os controles descritos na norma ABNT NBR ISO/IEC 27002. Esta norma é um dos documentos da Associação Brasileira de Normas Técnicas, que compõem a série 27000, a qual trata especificamente sobre segurança da informação. A norma é aplicável para todo o ambiente computacional de uma organização, desde as instalações físicas como cabamentos, até detalhes em nível de *software*.

A implementação das regras de *firewall* é sugerida através da ferramenta *iptables*, devido a sua utilização na maioria das distribuições Linux conhecidas.

A ferramenta *route*, encontrada na maioria das distribuições, é

utilizada para definir a tabela de roteamento, porém não provê opções para balanceamento de carga. Por esta razão, é proposto a implementação da tabela de roteamento utilizando a ferramenta *iproute*, a qual substitui plenamente a ferramenta *route*, além de prover as opções necessários para habilitar o balanceamento de carga.

1.4. Metodologia

Afim de observar o funcionamento e resultados finais em um ambiente real, duas empresas permitiram a implementação dos controles descritos nesta monografia, permitindo ainda a publicação dos resultados obtidos conforme as autorizações Anexo A e B.

A empresa CONTABILIDADE DORIVAL MACHADO E FILHOS possui uma rede com aproximadamente vinte computadores, entre terminais, servidor de dados e uma máquina específica para *firewall*. Este ambiente possui ainda duas conexões externas de internet com provedores diferentes, sendo a utilização de *link* alternada manualmente, deixando sempre uma das conexões ociosa. Este ambiente passa a ser denominado “caso A”.

A instituição FUNDAÇÃO EDUCACIONAL COMUNITÁRIA DE SÃO SEBASTIÃO DO PARAÍSO (LIBERTAS – FACULDADES INTEGRADAS), possui uma rede com aproximadamente duzentos e cinquenta computadores, incluindo servidores de dados e uma máquina específica para *firewall*. Este ambiente passa a ser denominado como “caso B”.

No cenário inicial em ambos os casos, a máquina *firewall* era

administrada de forma terceirizada pela própria empresa provedora de internet. Desta forma não se tinha um controle total das regras de *firewall* implementadas. Outro fator relevante é que não havia nenhum procedimento de *hardening* realizado, estando os sistemas operacionais e aplicações instalados de forma padrão, sem qualquer proteção adicional em se falando de segurança da informação.

1.5. Estrutura dos capítulos

O capítulo 2 objetiva fundamentar teoricamente sobre as tecnologias de *firewall* que envolvem esta monografia, descrevendo conceitos, tipos de *firewall*, utilização de *firewall* na camada de aplicação, além de detalhar um pouco sobre ferramentas utilizadas como `iptables` e `iproute`.

O capítulo 3 descreve o foco principal deste trabalho que é uma proposta de *hardening* baseado na norma ABNT NBR ISO/IEC 27002 para máquina *firewall* utilizando na distribuição linux `Debian`. São descritas ainda as propostas de implementação para adequação à norma, bem como uma sugestão de uma tabela de disposição regular, ou seja, uma ordem lógica para implementação dos controles.

O capítulo 4 refere-se exclusivamente sobre as regras de *firewall* implementadas através de `iptables`, observando também a conformidade com a norma citada.

O capítulo 5 descreve uma proposta de balanceamento de carga para um ambiente onde se tem duas conexões externas de internet que chegam a um mesmo *firewall*, o qual faz a ligação com a rede interna.

O capítulo 6 apresenta resultados obtidos com a implementação desta monografia em dois ambientes reais, sendo cada um, uma realidade empresarial diferente.

O capítulo 7 é a conclusão final deste trabalho, descrevendo os resultados obtidos e propondo trabalhos futuros a serem iniciados a partir desta monografia.

Capítulo 2

Fundamentação teórica sobre tecnologia de *Firewall*

2.1. *Firewall*

O Termo *Firewall* refere-se a um ponto de controle de segurança na fronteira entre duas redes (PALU, 2005). Este controle permite inspecionar o tráfego entre as redes, bloqueando ou aceitando os pacotes de acordo com as regras previamente implementadas por alguma ferramenta (Figura 1).

A implementação destas regras pode ser feita por várias ferramentas, dentre elas o IPFW e PFsense no FreeBSD, Packet Filter no OpenBSD e Netfilter no Linux. Esta última, através da interface iptables, é objeto de estudo desta monografia.

Existem dois tipos de *firewall* (TLDP, 2000):

- **filtro de pacotes:** Cada pacote é filtrado através de informações como o tipo de protocolo, endereço de destino ou origem e portas. Esta filtragem é feita através de regras que podem definir um ou mais quesitos ao mesmo tempo, como por exemplo porta e IP de destino.
- **servidor de proxy:** O *proxy* é um intermediador de conexões sendo a forma mais utilizada o *proxy* para conexões HTTP. O *software* faz armazenamento temporário dos dados acessados e sua principal vantagem é a melhoria de velocidade devido a amenização de tráfego dos acessos à internet (FERREIRA, 2003). As requisições vindas da rede interna, na maioria das

vezes são satisfeitas com os dados já armazenados no servidor *proxy*, liberando a banda externa para requisições de sites ainda não armazenados ou outros serviços que não utilizem *proxy*.

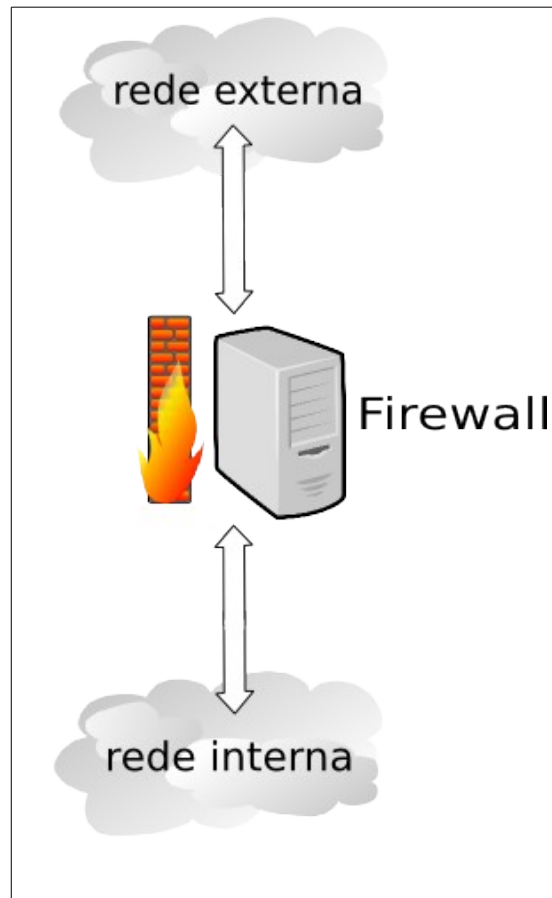


Figura 1: *firewall*

2.2. Firewall para a camada sete

A camada sete refere-se à camada de aplicação do modelo OSI, que

corresponde à camada quatro do modelo TCP/IP, tratando diretamente o conteúdo dos pacotes. Com o *firewall* atuando também nesta camada, é possível por exemplo bloquear aplicações difíceis de se controlar via IP ou porta, como é o caso do mensageiro instantâneo MSN.

Existem várias ferramentas para esta finalidade como o IPP2P, *Ourmon*, HiPPiE e o L7-Filter, sendo este último utilizado nesta monografia.

O L7-Filter é um classificador instalado através de um *patch* ao Iptables, funcionando como um módulo extra para tratamento da camada de aplicação quando invocado em alguma regra de filtragem (L7-FILTER, 2008).

2.3. Balanceamento de carga

É possível fazer o balanceamento de carga de uma banda de conexão, definindo a quantidade utilizada por cada máquina. Esta forma é muito utilizada em provedores de *internet* que através de ferramentas CBQ, definem a quantidade de *bits* por segundo que é liberada para cada cliente. Também pode ser utilizada dentro de uma organização afim de definir prioridades de uso para navegação, transferência de arquivos, entre outros fatores.

Existe a situação em que a máquina *firewall* possui mais de um *link* de saída para a internet, e deseja balancear o seu uso para as máquinas da rede interna, situação a qual é abordada nesta monografia conforme a Figura 2. Neste caso o balanceamento é feito nas requisições dos usuários para a rede externa, fazendo com que sejam utilizados todos os *link*, sem sobrecarga a nenhum deles. Um recurso adicional é que pode-se definir que requisições de uma máquina específica saia por determinado *link*, utilizando para isso o comando `ip rule`.

Este recurso é útil para uso, durante períodos de manutenção de um dos *link*.

Outro recurso que deve estar presente em um ambiente com balanceamento, é que um *link* venha a assumir totalmente o tráfego caso outros venham a falhar.

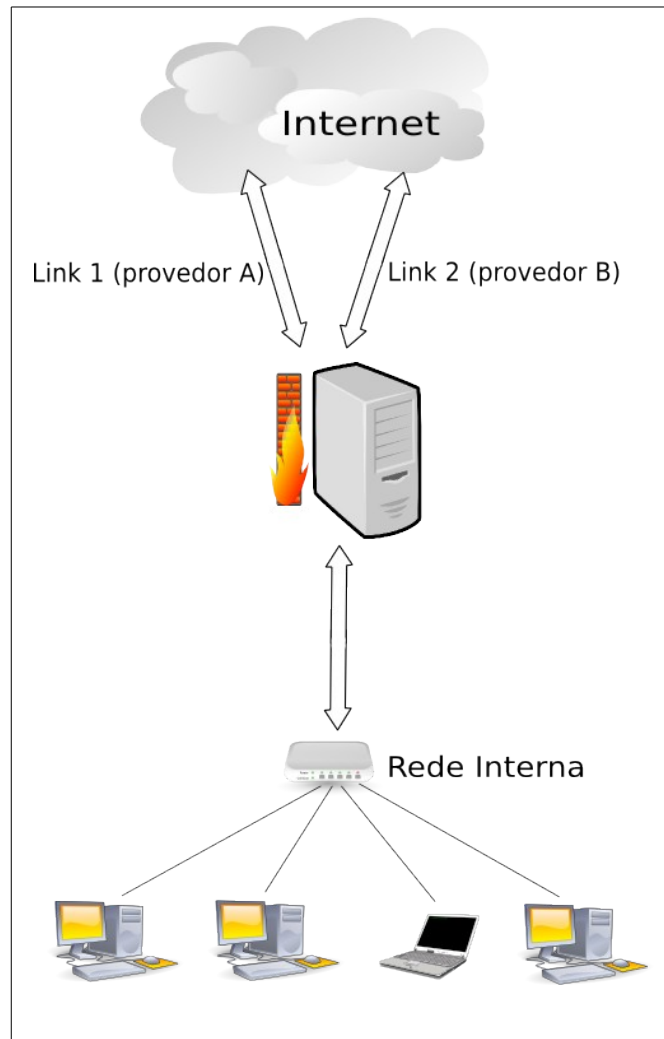


Figura 2: ambiente com *firewall* recebendo dois *link* externos

2.4. Iptables

O `netfilter` é uma ferramenta de filtragem de pacotes incluso na série de kernel 2.4 e 2.6 do Linux (NETFILTER, 2008). A configuração do `netfilter` é feita através de uma interface de camada de usuário denominada `Iptables`. Por esta ferramenta define-se as regras de bloqueio e liberação dos pacotes que passam pela máquina. É de praxe que a implementação destas regras seja feita por meio de um *script* afim de recuperá-las durante o reinício do sistema ou quando necessário.

O `Iptables` trabalha com três tabelas chamadas *filter*, NAT e *mangle*, sendo a primeira a tabela padrão (PALU, 2005).

A tabela *filter* refere-se a filtragem padrão, contendo as *chains* INPUT, OUTPUT e FORWARD, correspondendo respectivamente a entrada de pacotes na própria máquina, saída de pacotes da própria máquina e repasse de pacotes para outras máquinas.

A tabela NAT, refere-se a tradução de endereços de uma rede para outra, contendo as *chains* PREROUTING, POSTROUTING e OUTPUT. A *chain* PREROUTING corresponde a alterações nos pacotes vindos de uma rede antes do roteamento para outra rede. A *chain* POSTROUTING corresponde a alterações nos pacotes vindos de uma rede e já roteados e prontos para saírem para outra rede. Por fim a *chain* OUTPUT, corresponde a saída de pacotes da própria máquina e que precisam de alguma alteração antes desta saída.

Por fim, a tabela *mangle* refere-se a alterações especiais nos pacotes para então repassá-los.

A tabela 1 demonstra as ações que são realizadas sobre os pacotes que atendem a uma determinada regra (FREITAS 2002).

Tabela 1: ações realizadas pelo `iptables`

Nome	Descrição
ACCEPT	Aceite do pacote
DROP	Negação do pacote
REJECT	Rejeição do pacote, gerando um pacote de resposta
MASQUERADE	Conversão de endereço
LOG	Registro de LOG da passagem por uma regra
SNAT	Alteração do endereço de origem
DNAT	Alteração do endereço de destino

2.5. Iproute

O pacote `iproute` realiza várias funções em relação a configuração de redes, substituindo comandos como `arp`, `ifconfig` e `route` (LOUREIRO 2004) e permitindo assim a visualização e manipulação de rotas e dispositivos de rede.

O comando `ip`, pertencente ao pacote `iproute`, é quem traz estas funcionalidades (FREITAS, 2002), passando argumentos apropriados para os objetos conforme descrição na tabela 2.

Dentre as funcionalidades do `iproute`, está a criação de várias tabelas de roteamento, as quais são denominadas no arquivo `/etc/iproute2/rt_tables`. Estas tabelas recebem um identificador (ID) que vai de 0 a 255, sendo que 0 e 253 a 255 são identificadores reservados para o sistema (LOUREIRO, 2004), ficando o restante livre para criação de novas tabelas, conforme ilustrado na Figura 3. Após criadas as novas tabelas, ainda deverão ser adicionados através do comando `ip route`, os roteamentos para as redes existentes. Por fim estas tabelas devem ser referenciadas por

alguma regra através do comando `ip rule`, caso contrário não poderão fazer nenhum efeito no sistema. Este último comando é quem define por qual tabela de roteamento os pacotes deverão passar.

Tabela 2: objetos de configuração do comando `ip`

Objeto	Descrição
<code>link</code>	interface física
<code>addr</code>	endereço lógico
<code>route</code>	roteamento
<code>maddr</code>	endereço lógico de multicast
<code>mroute</code>	roteamento multicast
<code>tunnel</code>	túnel de protocolo
<code>neigh</code>	tabela ARP
<code>rule</code>	regras de roteamento
<code>monitor</code>	monitoração dos demais objetos

255	local
254	main
253	default
202	rota2
201	rota1

Figura 3: arquivo `/etc/iproute2/rt_tables`

Capítulo 3

Proposta de *hardening* para um sistema *firewall* baseado em Debian

3.1. Sobre a família de regras ABNT NBR ISO/IEC 27000

O primeiro padrão de segurança da informação do qual originou todos os demais, é o BS 7799, estando dividido em duas partes.

A primeira parte com nome de BS 7799-1 e denominação “Código de prática para gerenciamento de segurança da informação” foi criada em 1995, e tinha por objetivo estabelecer um conjunto detalhado dos controles para gerenciamento da segurança da informação. Devido a sua eficiência e trabalho similar à certificação ISO, em 2000 tornou-se o padrão ISO 17799 [KNOWLEDGELEADER, 2003]. Finalmente em 2005 a ISO 17799 tornou-se a ISO 27002, então traduzida e publicada pela ABNT através da norma NBR ISO/IEC 27002. De acordo com (ABNT, 2008), o conteúdo técnico da NBR ISO/IEC 17799 é idêntico ao da NBR ISO/IEC 27002, tendo sido alterado apenas a numeração da série. Uma comparação e descrição de conteúdos é demonstrado na tabela 3.

A NBR ISO/IEC 27002 é um código de prática, que descreve controles e objetivos de controles para a gestão de segurança da informação. É o documento utilizado por uma instituição com o intuito de buscar conformidade com a ISO no quesito segurança da informação.

A segunda parte com nome de BS 7799-2 e denominação

“Especificações para gerenciamento de sistemas de segurança da informação” foi criada em 2002, e tinha por objetivo um gerenciamento do sistema de segurança da informação proposto na BS 7799-1 (ISO 17799). Em 2005 tornou-se o padrão ISO 27001 (KNOWLEDGELEADER, 2003), traduzido e publicado pela ABNT através da norma NBR ISO/IEC 27001. Esta tem por objetivo:

“(...) prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação.” (ISO 27001, 2006).

Os objetivos de controle e controles descritos na ABNT NBR ISO/IEC 27001, são derivados diretamente da ABNT NBR ISO/IEC 27002. Assim, a norma ABNT NBR ISO/IEC 27001 é o documento utilizado por um auditor afim de comprovar os controles da NBR ISO/IEC 27002 implementados em uma instituição, a qual tem por objetivo a certificação ISO 27001.

Em 2005 surge a BS7799-3 (STANDARDS, 2005) com denominação “Guia para gerenciamento de riscos em segurança da informação”, a qual em 2008 tornou-se ISO 27005 (ISO, 2008), publicada pela ABNT através da NBR ISO/IEC 27005.

Segundo (ISO, 2008), em 2007 surgiu o padrão ISO 27006 denominado “Exigências para os corpos que fornecem o exame e a certificação de sistemas de gestão da segurança da informação”, sendo destinado à empresas que fornecem certificação em segurança da informação, porém não é o foco desta monografia.

Toda esta linha cronológica pode ser melhor visualizada através da Figura 4.

Tabela 3: comparação e descrição de conteúdos das normas ISO e BS

Norma ISO	Descrição	Equivalência com norma BS
ISO 27002	Código de prática para a gestão da segurança da informação	BS 7799-1 (ISO 17799)
ISO 27001	Sistemas de gestão de segurança da informação - Requisitos	BS 7799-2
ISO 27005	Gestão de riscos de segurança da informação	BS 7799-3
ISO 27006	Exigências para os corpos que fornecem o exame e a certificação de sistemas de gestão da segurança da informação	não tem

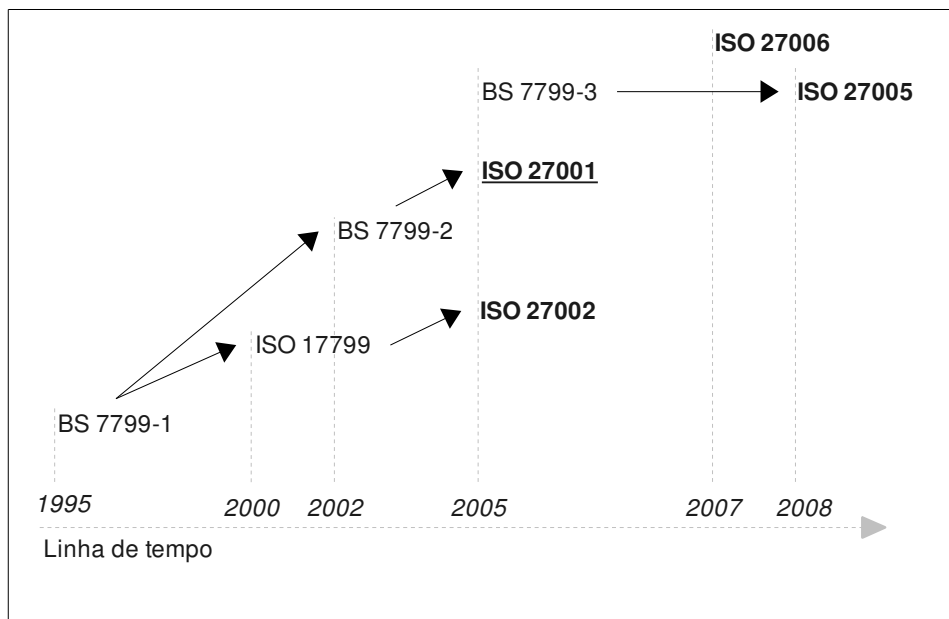


Figura 4: linha cronológica do padrão ISO 27000

No Brasil, a série 27000 da ISO, é o único padrão de segurança da informação encontrado, motivando assim a adoção desta norma para a

implementação desta monografia, observando os controles descritos na ABNT NBR ISO/IEC 27002, para adequação com a ABNT NBR ISO/IEC 27001, de agora em diante referenciada pelo nome ISO 27001.

3.2. O processo de *hardening*

Para estabelecer a conformidade com a ISO 27001, este documento propõe um processo de *hardening*, ou seja, um refinamento do sistema, observando os requisitos propostos pela norma. Este procedimento é embasado também no princípio do menor privilégio (SALTZER, 1975).

“Menor privilégio: cada programa e cada usuário do sistema deve operar usando o menor conjunto de privilégios necessários para completar uma operação.” (SALTZER, 1975)

Nem todos os os controles apresentados na ISO 27001 são aplicáveis especificamente à máquina *firewall*, assim esta monografia busca atender somente os controles inerentes ao *hardening* desta máquina.

Para que estes controles funcionem adequadamente, é necessário um processo contínuo de verificação das implementações de controle realizadas. Este processo é denominado na própria norma como PDCA (Figura 5) sendo composto de um círculo contínuo das etapas descritas na tabela 4 (ISO27001, 2006).

A atuação desta proposta de *hardening* está na camada de usuário, tecnicamente conhecida como *userland*, estando passível de uma falha através do ID 0, ou seja, quando o usuário consegue nível privilegiado, passando então a

atuar como `root`. Esta falha pode ser corrigida atuando em nível de *kernel*, o qual não é o foco desta monografia.

Tabela 4: descrição das etapas do modelo PDCA da ISO 27001

Etapa	Descrição
Plan (planejar)	Estabelecer a política, procedimentos, processos e objetivos
Do (fazer)	Implementar o que foi planejado
Check (checar)	Avaliar a implementação executada,
Act (agir)	Manter e melhorar a segurança baseando-se na checagem anterior, executando ações corretivas e preventivas quando necessário

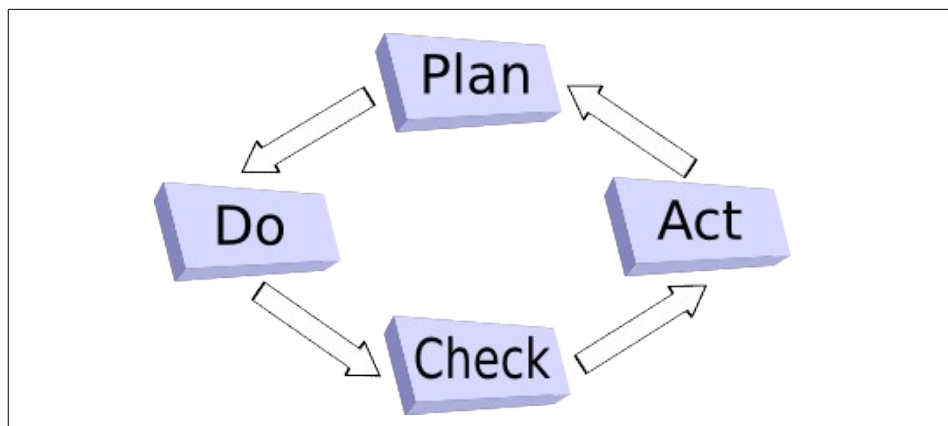


Figura 5: modelo PDCA de acordo com a ISO 27001

3.3. Disposição regular das etapas do *hardening*

Para fins de organização lógica da implementação dos controles sugeridos na ISO 27001, esta monografia estabelece uma linha de base (tabela 5) para servir como referência de disposição regular, isto é, uma ordem adequada de implementação dos controles que serão descritos à frente.

Esta tabela tem como referência o modelo proposto pelo Mitre (MITRE, 2008) para organizar cronologicamente os procedimentos do Guia para configuração segura de *Red Hat Enterprise Linux 5* (NSA, 2008) da Agência Nacional de Segurança dos Estados Unidos da América.

3.3.1 Controles da ISO 27001 inerentes à política de segurança

Toda a implementação de controles, deve integrar a documentação da política de segurança, a qual deve ser aprovada pela direção e levada ao conhecimento das pessoas envolvidas, com exceção de detalhes técnicos como nome de ferramentas utilizadas ou outra informação que favoreça um possível ataque por engenharia social.

Desta forma, faz-se atender ao item A.5.1.1 “Documentação da política de segurança da informação”.

Deverá ainda, ser realizada uma análise crítica dos controles implementados em intervalos planejados. Este procedimento deve ser feito pelo proprietário da máquina *firewall*, bem como em um processo de auditoria. Isso se faz necessário para assegurar a contínua eficácia do sistema de segurança da informação, atendendo assim o item A.5.1.2 “Análise crítica da política de segurança da informação”.

Tabela 5: proposta de ordem lógica para realização das etapas do hardening

Área de atuação	Controle recomendado pela ISO 27001 (item)	Procedimento prático sugerido nesta proposta (item)
Segurança física	A.9.1.1 A.9.1.6 A.9.2.1 A.9.2.2 A.9.2.3	3.3.4
Manuseio de mídias	A.10.7.1	3.3.8
Responsabilidade de usuários	A.11.3	3.3.11
Gestão de ativos	A.7.1	3.3.3
Aquisição, desenvolvimento e manutenção de sistemas de informação	A.12.1.1 A.12.4.1	3.3.14
Gerenciamento de acesso do usuário	A.11.3	3.3.10
Acesso ao sistema operacional	A.11.2	3.3.12
Trabalho Remoto	A.11.7	3.3.13
Monitoramento	A.10.10.1 A.10.10.2 A.10.10.3 A.10.10.4 A.10.10.5 A.10.10.6	3.3.9
Cópia de segurança	A.10.5.1	3.3.7
Gestão de incidentes de segurança da informação	A.13.1.1 A.13.1.2 A.13.2	3.3.16
Gestão de continuidade de negócios	A.14	3.3.17
Segurança dos arquivos do sistema	A.12.4.1	3.3.15
Proteção contra códigos maliciosos	A.10.4.1	3.3.6
Gerenciamento das operações de comunicações	A.10.1.1	3.3.5
Conformidade	A.15.1	3.3.18
Auditoria de sistemas de informação	A.15.3	3.3.19
Política de segurança	A.5.1.1 A.5.1.2	3.3.1
Organização da segurança da informação	A.6.1.1 A.6.1.3	3.3.2

3.3.2 Controles da ISO 27001 inerentes à organização da segurança da informação

A Direção deve apoiar ativamente a segurança da informação, demonstrando de forma clara o seu comprometimento através de documento assinado e anexado à política de segurança, atendendo assim o ítem A.6.1.1 “Comprometimento da direção com a segurança da informação”.

A responsabilidade da segurança da informação perante a máquina *firewall*, deve ser do usuário proprietário. Essa informação deve estar disposta claramente no documento da política de segurança. Desta forma é atendido o ítem A.6.1.3 “Atribuição de responsabilidades para a segurança da informação”.

3.3.3 Controles da ISO 27001 inerentes à gestão de ativos

Além do inventário da máquina *firewall* e periféricos necessários para o seu funcionamento, deve-se estabelecer o proprietário, ou seja, a pessoa com responsabilidade pelo equipamento.

Deve-se estabelecer também, o uso aceitável do equipamento por parte do proprietário, isto é, definir de forma clara a utilização a que se destina a máquina *firewall*, não podendo ser utilizada para outra finalidade. Desta forma, é atendido o ítem A.7.1 “Responsabilidade pelos ativos”.

3.3.4 Controles da ISO 27001 inerentes à segurança física

O equipamento deve estar em um perímetro de segurança pré-estabelecido, sem acesso direto ao público, atendendo assim os ítem A.9.1.1

“Segurança física e do ambiente” e A.9.1.6 “Acesso do público”.

O perímetro de segurança pré-estabelecido, deve ser um local protegido de possíveis ameaças do meio ambiente, proteção contra falta de eletricidade através do uso *nobreak*, cabeamento protegido contra interceptações utilizando conduítes metálicos. Por fim evitar ao máximo oportunidades de acesso de pessoas não autorizadas, atendendo assim os itens A.9.2.1 “Instalação e proteção do equipamento”, A.9.2.2 “Utilidades” e A.9.2.3 “Segurança do cabeamento”.

3.3.5. Controles da ISO 27001 inerentes ao gerenciamento das operações e comunicações

Os procedimentos de operação, administração e uso da máquina *firewall*, devem ser documentados e atualizados sempre que necessário, sendo assim disponíveis quando necessário. O proprietário deve estabelecer uma política de uso com instruções técnicas de uso do equipamento, bem como um histórico de ações relevantes já realizadas, como alteração de IPs, portas, manutenção ou troca de componentes físicos da máquina, entre outros. Desta forma atende-se o item A.10.1.1 “Documentação dos procedimentos de operação”.

3.3.6. Controles da ISO 27001 inerentes a proteção contra códigos maliciosos

A inserção de códigos maliciosos é um dos recursos utilizados pelo potencial invasor, afim de garantir futuros acessos ao sistema. Pode ser feito de várias formas, sendo um exemplo a utilização *rootkits*, que são versões alteradas

de programas convencionais, os quais propiciam ao usuário, privilégios de `root` (TEIXEIRA, 2005).

O invasor pode aproveitar-se ainda do recurso de *set user id (Suid Bit)*, o qual faz com que um programa seja executado com permissão do seu dono ao invés do usuário ativo, procurando então arquivos estratégicos do sistema como um `bash` por exemplo (MELO, 2006). Como esta norma embasa-se no conceito de menor privilégio, não é interessante manter arquivos com *suidbit* no sistema.

Outro recurso muito eficiente utilizado pelo potencial invasor, é a permissão na partição para executar arquivos binários ou scripts executáveis, possibilitando ao mesmo executar qualquer aplicação do sistema ou inserida por ele mesmo.

Este problema pode ser eliminado pela raiz, através da implementação segura do arquivo `/etc/fstab` (Figura 6).

<code>/dev/hda1</code>	<code>/boot</code>	<code>ext3</code>	<code>defaults,nosuid</code>	<code>0 2</code>
<code>/dev/hda3</code>	<code>/home</code>	<code>ext3</code>	<code>defaults,nosuid,noexec</code>	<code>0 2</code>
<code>/dev/hda5</code>	<code>/var</code>	<code>ext3</code>	<code>defaults,nosuid,noexec</code>	<code>0 2</code>
<code>/dev/hda7</code>	<code>/tmp</code>	<code>ext3</code>	<code>defaults,nosuid,noexec</code>	<code>0 2</code>

Figura 6: trecho do arquivo `/etc/fstab`

Convém ainda a implantação de um controle de integridade dos arquivos, afim de prevenir a inserção de códigos maliciosos, seja por alteração de arquivos já existentes no sistema, bem como a instalação de novas aplicações. Este controle de integridade pode ser feito por ferramentas como *AIDE*, *Osiris*, *Tripwire*, *Integrit* entre outras.

Através de agendamento pelo `cron`, esta proposta sugere uma verificação diária na máquina *firewall*, sugerindo ainda a utilização da

ferramenta *Osiris*. Conforme análise de (DOMINGUES, 2003), o qual faz uma comparação entre as quatro ferramentas de integridade citadas, o *Osiris* é recomendado para situações onde é necessário a verificação de integridade de arquivos de forma rápida, enquadrando-se bem no caso de verificação diária, afim de não comprometer o desempenho da máquina. O *Osiris* tem ainda a vantagem de funcionar em modo cliente servidor, onde a verificação pode partir de outra máquina habilitada para tal finalidade.

Por fim, ainda é sugerido a utilização da ferramenta *chkrootkit*, a qual é uma aplicação exclusivamente para detecção de rootkits instalados na máquina. Esta ferramenta pode ser utilizada a intervalos regulares, bem como em um processo de auditoria a ser descrito mais adiante.

Este conjunto de procedimentos possibilitam atender ao item A.10.4.1 “Controle contra códigos maliciosos”.

3.3.7. Controles da ISO 27001 inerentes a cópias de segurança

Deve ser realizado uma cópia de segurança dos arquivos de configuração afim de garantir uma restauração rápida em caso de não disponibilidade do equipamento.

A utilização de um *script* de automação para este procedimento conforme sugerido através do Apêndice E, agiliza o trabalho e impede falha humana. É importante lembrar que devem ser previamente geradas as chaves de *ssh* para que o *script* realize a operação sem interferência humana.

Uma vez copiado o arquivo de *backup* para a outra máquina ainda dentro da instituição, cabe ao administrador da rede providenciar o transporte físico do mesmo para outra localidade fora da instituição. Desta forma atende-se o item

A.10.5.1 “Cópias de segurança das informações”.

3.3.8. Controles da ISO 27001 inerentes a manuseio de mídias

A utilização de mídias removíveis em máquinas firewall é desnecessário. Assim, convém desabilitar totalmente o acesso por mídias removíveis como entradas USB, drive de disquete e CD, ou similares. Esse procedimento pode ser realizado através da desconexão física dos dispositivos ou através de opções de inicialização da placa mãe. Desta forma, é atendido o ítem A.10.7.1 “Gerenciamento de mídias removíveis”.

É importante saber que para adotar o procedimento de interferência física, a máquina já deve estar inventariada e com proprietário definido para realizar tal operação.

3.3.9. Controles da ISO 27001 inerentes a monitoramento

O monitoramento é um recurso fundamental o qual auxilia muito o administrador de redes na identificação e resolução de problemas. Deve ser realizado um registro de LOG da utilização da máquina, além de registro dos dados que por ela passam.

Para monitorar o uso da própria máquina *firewall*, sugere-se o uso da *Snoopy Logger*, que registra todos os comandos executados seja pelo `root` como por todos os demais usuários habilitados no sistema (Figura 7). Esta ferramenta em conjunto com o *syslog*, o qual é parte integrante da instalação padrão do Debian, possibilitam uma boa cobertura de tudo o que é feito na máquina. Pode-se optar por outras ferramentas de LOG de preferência, desde que estas possibilitem um registro de LOG íntegro.

```

Jul 11 00:05:05 dorival-firewall snoopy[4651]: [unknown, uid:0 sid:4619]: ip rule
Jul 11 00:05:05 dorival-firewall snoopy[4654]: [unknown, uid:0 sid:4619]: ip rule
Jul 11 00:05:05 dorival-firewall snoopy[4655]: [unknown, uid:0 sid:4619]: grep 189.43.151.19
Jul 11 00:05:05 dorival-firewall CRON[4617]: (pam_unix) session closed for user root
Jul 11 00:05:56 dorival-firewall snoopy[4656]: [djunior, uid:0 sid:4359]: ls --color=auto -lh
Jul 11 00:06:06 dorival-firewall snoopy[4657]: [djunior, uid:0 sid:4359]: md5sum squid.conf.old
Jul 11 00:06:14 dorival-firewall su[4503]: (pam_unix) session closed for user root
Jul 11 00:06:15 dorival-firewall sshd[4358]: (pam_unix) session closed for user djunior
Jul 11 00:07:09 dorival-firewall snoopy[4659]: [djunior, uid:0 sid:32332]: cat /var/log/auth.log
Jul 11 00:07:20 dorival-firewall snoopy[4660]: [djunior, uid:0 sid:32332]: tail /var/log/auth.log

```

Figura 7: trecho de monitoramento registrado pelo Snoopy Logger.

Para monitorar os dados que passam pela máquina, propõe-se utilizar o Squid auxiliado pelo SARG, pelo fato da máquina em questão ser um *proxy* transparente. Assim, através da personalização da saída do LOG arquivo de configuração do Squid (Figura 8), é definido o registro de apenas informações relevantes para a empresa (Figura 9).

```

logformat MEU_LOG %t1 | %>a | %Ss | %<A | %ru %rm | %Hs
cache_access_log /var/log/squid/gerencia.log MEU_LOG

```

Figura 8: linhas inseridas no squid.conf para geração do LOG personalizado

```

10/Jul/2008:23:55:12 -0300 | 192.168.100.97 | TCP_MISS | 161.148.231.100 |
http://www.receita.fazenda.gov.br/ GET | 200
10/Jul/2008:23:55:13 -0300 | 192.168.100.97 | TCP_REFRESH_MISS | 161.148.231.100 |
http://www.receita.fazenda.gov.br/js/SRFMenu.js GET | 200
10/Jul/2008:23:55:15 -0300 | 192.168.100.97 | TCP_MEM_HIT | - |
http://www.terra.com.br/favicon.ico GET | 200

```

Figura 9: trecho de LOG personalizado gerado pelo Squid

Implementando todos estes monitoramentos atende-se aos ítems A.10.10.1 “Registros de auditoria”, A.10.10.2 “Monitoramento do uso do sistema” e A.10.10.4 “Registros de administrador e operador” e A.10.10.5 “Registros de falhas”.

O item A.10.10.3 “Proteção das informações dos registros” é atendido através da utilização do *Osiris* como controle de integridade de arquivo.

Ainda na questão do monitoramento, é necessário uma sincronização de todos os relógios do sistema, afim de manter a confiabilidade nos horários registrados em LOG, e assim atender o item A.10.10.6 “Sincronização dos relógios”. Para tanto, sugere-se a sincronização periódica com um servidor NTP público conforme o Apêndice F.

3.3.10. Controles da ISO 27001 inerentes ao gerenciamento de acesso de usuário

Em uma máquina *firewall*, convém cadastrar apenas os usuários necessários à administração do sistema. A máquina *firewall* requer além do *root*, um usuário normal, pelo qual se possa fazer o *login* no terminal ou fazer acesso remoto.

Sendo esta máquina também um *proxy* transparente, admite-se a possibilidade de habilitar um outro usuário para a administração do SARG via navegador através da rede interna. Como se trata de um usuário para administração remota e que não necessita de acesso no sistema operacional, deve-se eliminar o *shell* do mesmo, atendendo ao conceito do menor privilégio. Desta forma, é atendido o item A.11.2 “Gerenciamento de acesso do usuário”.

3.3.11. Controles da ISO 27001 inerentes a responsabilidade dos usuários

O usuário proprietário da máquina *firewall*, deve observar atentamente a

política de senha estabelecida pela empresa. Esta se resume a utilização de senhas fortes e não permitir o acesso às mesmas por parte de terceiros. Também deve ser adotado a política de tela limpa, omitindo ao máximo informações da máquina *firewall* para terceiros.

Estes procedimentos permitem atender o ítem A.11.3 “Responsabilidade dos usuários”.

3.3.12. Controles da ISO 27001 inerentes ao controle de acesso ao sistema operacional

O acesso ao sistema operacional, deve ser permitido somente a um usuário normal em especial e o *root*. Desta forma, é necessário um conjunto de procedimentos conforme a tabela 6, para então alcançar este objetivo de forma satisfatória e assim atender ao ítem A.11.2 “Gerenciamento de acesso do usuário”.

```
# autenticação requer que usuário seja do grupo admin
# (grupo previamente criado)
auth required pam_wheel.so group=admin
```

Figura 10: trecho do arquivo */etc/pam.d/su*

```
# o login tem como requisito o controle de horario
account requisite pam_time.so
```

Figura 11: trecho do arquivo */etc/pam.d/login*

```
# bloqueio de uso do "login" para o "root" a qualquer momento
login;*;root;!A10000-2359
```

Figura 12: trecho do arquivo */etc/pam.d/time.conf*

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/false
bin:x:2:2:bin:/bin:/bin/false
sys:x:3:3:sys:/dev:/bin/false
proxy:x:13:13:proxy:/bin:/bin/false
www-data:x:33:33:www-data:/var/www:/bin/false
identd:x:102:65534:./var/run/identd:/bin/false
djunior:x:1000:1000:DorivalJr,,,:/home/djunior:/bin/b
```

Figura 13: trecho do `/etc/passwd` onde apenas root e usuário estratégico possuem um shell válido

```
# The DSHELL variable specifies the default login shell on your
# system.
DSHELL=/bin/false
```

Figura 14: trecho do arquivo `/etc/adduser.conf` definindo um caminho inválido de *shell* para novos usuários

```
# ca:12345:ctrlaltdel:/bin/echo "opcao nao habilitada"
```

Figura 15: trecho do arquivo `/etc/inittab` referente a desabilitação do CTRL+ALT+DEL

```
Port 62333
PermitRootLogin no
```

Figura 16: trecho do arquivo `/etc/ssh/sshd_config` referente a desabilitação de *login* remoto do root e alteração da porta ssh

Tabela 6: procedimentos para controle de reforço no acesso ao sistema operacional

Procedimento	Sugestão de implementação prática
- reforço no sistema de <i>login</i> local.	Criação de um usuário normal para a finalidade de <i>login</i> no terminal. Uma vez logado, este usuário alterna-se para <i>root</i> através do <i>su</i> . Deve-se ainda providenciar para que apenas este usuário tenha permissão de uso do <i>su</i> . (Figura 10). Complementando, esta proposta sugere o bloqueio de <i>login</i> do <i>root</i> diretamente no terminal. Todas estas implementações podem ser realizadas através do PAM (Figura 11 e 12).
- remoção do <i>shell</i> de todos os usuários, com exceção do <i>root</i> e usuário normal para fins de <i>login</i> , impedindo o acesso indevido ao sistema operacional.	Remoção de <i>shell</i> dos usuários em <i>/etc/passwd</i> (Figura 13) e alteração junto ao <i>/etc/adduser.conf</i> para que possíveis novos usuários recebam um <i>shell</i> inválido (Figura 14). A remoção deve ser realizada inclusive para usuários de sistema.
- remoção de programas desnecessários ao sistema.	Primeiro obtém-se a lista de pacotes instalados através do comando <code>dpkg -l</code> . Em seguida, após análise, dos pacotes, remove-se o que não é necessário ao funcionamento do sistema e do <i>firewall</i> . Esta remoção implica também em programas clientes, os quais não precisam estar presentes na máquina caso não sejam realmente necessários. Um exemplo é o utilitário <i>wget</i> que faz <i>download</i> sem interação humana (MELO, 2006).
- desabilitação de reinicialização via terminal.	Desabilitação da combinação de teclas CTRL+ALT+DEL para reinício da máquina, através de edição do arquivo <i>/etc/inittab</i> (Figura 15).
- reforço no sistema de <i>login</i> remoto.	Sugere-se que o <i>login</i> remoto seja feito apenas por <i>ssh</i> , afim de garantir uma maior segurança. Na configuração do <i>ssh</i> , convém que seja desabilitado a opção de <i>login</i> remoto do <i>root</i> ; sugere-se ainda a alteração da porta <i>ssh</i> para uma outra porta de número alto, dificultando possíveis tentativas de força bruta na porta padrão (Figura 16).

3.3.13. Controles da ISO 27001 inerentes a computação móvel e trabalho e remoto

É de praxe o trabalho de administração de um *firewall* ser feito remotamente. Logo este acesso somente é aceitável através de conexões criptografadas. Sugere-se fortemente o uso de SSH, o qual criptografa toda a conexão, incluindo o nome e senha do usuário para *login*.

Com base no princípio do menor privilégio, o `root` deve ser impedido de realizar conexões remotas (Figura 16) através de configuração do próprio SSH. Para o acesso remoto, utiliza-se um usuário normal, o qual após estabelecer a conexão, e estando em um ambiente seguro, faz-se a mudança para usuário `root` através do `su`.

Para a administração do SARG via navegador, são necessários cuidados como não deixar senhas gravadas no computador de acesso, bem como utilizar um equipamento confiável e de uso próprio. Mesmo que a conexão seja segura através de protocolo `https`, deve-se evitar a administração a partir de computador de terceiros.

Desta forma é atendido o item A.11.7 “Computação móvel e trabalho remoto”.

3.3.14. Controles da ISO 27001 inerentes a aquisição, desenvolvimento e manutenção de sistemas de informação

É adotado como princípio nesta monografia, utilizar somente ferramentas *opensource* ou livre distribuição. Para a aquisição das mesmas, é sugerido o utilitário `apt-get`, desde que este utilize repositórios oficiais

Debian (Figura 17) ou a instalação manual de pacotes `.deb` adquiridos em *sites* oficiais. A utilização deste tipo de pacote, elimina a possibilidade de erros de compilação, que normalmente acontecem quando adquire-se código fonte para a instalação, além do tempo de instalação por pacotes ser consideravelmente mais rápido em relação a instalação por código fonte.

Em caso de aquisição de pacotes `.deb`, deve-se fazer uma verificação de integridade dos mesmos. A maioria dos projetos disponibilizam uma forma de checagem de integridade de arquivos para conferência após o *download*.

Estes procedimentos permitem atender aos ítem A.12.1.1 "Análise e especificação dos requisitos de segurança" e A.12.4.1 "Controle de softwares operacionais".

```
deb http://ftp.br.debian.org/debian/ etch main
deb http://security.debian.org/ etch/updates main contrib
```

Figura 17: arquivo `/etc/apt/sources.list` com repositórios oficiais Debian

3.3.15. Controles da ISO 27001 inerentes a segurança dos arquivos do sistema

Os mesmos procedimentos sugeridos anteriormente no sub ítem 3.3.14 deste documento, também atendem ao ítem A.12.4.1 "Controle de software operacional" o qual sugere que seja estabelecido um controle para instalação de programas, estabelecendo assim uma forma mais confiável de origem de arquivos de instalação.

3.3.16. Controles da ISO 27001 inerentes a gestão de incidentes de segurança da informação

A ISO 27001 define evento de segurança da informação como:

“Uma ocorrência identificada de um estado de sistema, serviço ou rede, indicando uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.” [ISO 27001, 2006]

Diante desta descrição, esta monografia sugere que qualquer evento de segurança da informação referente à máquina *firewall*, seja imediatamente relatada pelo proprietário à direção através de ofício com assinatura de protocolo. Caso o evento seja identificado primeiramente por outra pessoa da organização, este deve notificar imediatamente ao proprietário da máquina *firewall*, o qual se encarrega de notificar a direção, citando no ofício a pessoa e a forma de detecção do problema.

Estes procedimentos fazem produzir uma conformidade com os itens A.13.1.1. “Notificação de eventos de segurança da informação” e A.13.1.2 “Notificando fragilidades de segurança da informação”.

Uma vez notificadas as falhas ou fragilidades, cabe ao proprietário do *firewall*, proceder da forma mais rápida para sanar o problema detectado, uma vez que este tem total responsabilidade pela máquina. Ele deve ainda manter um relatório dos incidentes ocorridos afim de quantificar os dados para futuros monitoramentos mais específicos de uma falha.

Desta forma é estabelecida uma conformidade com o item A.13.2

“Gestão de incidentes de segurança da informação e melhorias”.

Esta etapa pode ainda ser amparada pela norma NBR ISO/IEC 27005, que trata exclusivamente sobre “Gestão de riscos de segurança da informação”.

3.3.17. Controles da ISO 27001 inerentes a gestão de continuidade do negócio

Para assegurar a retomada do *firewall* em tempo hábil em caso de problemas, sugere-se que seja mantido um backup dos arquivos de configuração de todas as ferramentas utilizadas, bem como uma máquina espelho, afim de impedir a interrupção prolongada em caso de falha física ou danificação em maior grau causado por uma invasão.

Os mesmos processos de notificação descritos na gestão de incidentes de segurança, também são cabíveis na gestão de continuidade do negócio.

Todos os eventos de segurança identificados e corrigidos, devem ser submetidos a testes afim de comprovar a eliminação do problema.

Desta forma é atendido o ítem A.14 “Gestão de continuidade do negócio”.

3.3.18 Controles da ISO 27001 inerentes a conformidade

O recurso de *proxy* transparente através da ferramenta SQUID, permite gerar e manter gravado um registro de tudo o que foi acessado através deste *firewall*. Assim, na política de segurança deve estar bem claro que a utilização

dos recursos de processamento da informação, são exclusivamente para propósitos empresariais, não sendo permitido o uso para fins ilícitos ou proibidos por Lei. A utilização fora deste padrão, passa a ser de responsabilidade do usuário. Esta instrução também se enquadra para o uso de correio eletrônico com domínio da empresa, proibindo ainda o uso de correio eletrônico de outros domínios para os fins organizacionais.

Como esta monografia sugere a utilização de ferramentas *opensource* ou livre distribuição, não há possibilidade de problemas com direitos de propriedade intelectual.

Desta forma, é atendido o item A.15.1 “Conformidade com requisitos legais” que estabelece que sejam definidos controles para evitar a violação de lei criminal ou civil, bem como as obrigações contratuais da empresa e a política de segurança.

3.3.19 Controles da ISO 27001 inerentes a auditoria de sistemas de informação

É sugerido que a equipe ou pessoa responsável pela auditoria, seja terceirizado ou não tenha nenhum vínculo de utilização da máquina *firewall*, garantindo um resultado não tendencioso. Em caso de serviço terceirizado, é importante observar a idoneidade da pessoa ou equipe escolhida para realizar a auditoria.

Todo o procedimento de auditoria, incluindo arquivos a serem verificados e procedimentos utilizados devem ser previamente documentados através de contrato assinado entre as partes.

Para auxiliar no processo de auditoria, esta monografia sugere a ferramenta *autopsy*, a qual segundo (TEIXEIRA, 2005) faz procura por

evidências utilizando diversas técnicas aceitáveis para a adequação à ISO 27001, como linha de tempo de ações, listagem de arquivos e diretórios incluindo os apagados, entre outros.

A ferramenta `chkrootkit` anteriormente indicada, também é aceitável para auxiliar no processo de auditoria.

Estes procedimentos permitem atender ao item A.15.3 “Considerações quanto à auditoria de sistemas de informação”.

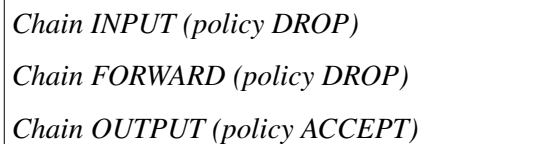
Capítulo 4

Firewall

Foi desenvolvido um *script* (Apendice B) intitulado “Mirar Firewall” com o intuito de atender ao item A.11.3 “Controle de acesso à rede” que tem por objetivo “Prevenir acesso não autorizado aos serviços de rede” (ISO 27001, 2006).

As regras de *firewall* propostas através deste Apêndice B, incluem repasse entre redes, bloqueio e liberação de portas e IPs, implementação de controle na camada de aplicação (camada sete do modelo OSI), bem como recursos de NAT e PAT.

Baseando no conceito de menor privilégio, sugere-se uma política restritiva (Figura 18), liberando somente o que for necessário. Havendo um bom tratamento nas regras de INPUT ou FORWARD, pode-se optar pela liberação do OUTPUT.



```
Chain INPUT (policy DROP)
Chain FORWARD (policy DROP)
Chain OUTPUT (policy ACCEPT)
```

Figura 18: política restritiva no Iptables

4.1 Regras básicas para roteamento

As regras básicas de roteamento permitem em primeiro lugar, o funcionamento da própria máquina e seus serviços através de liberação de

entrada de pacotes por *loopback* ou pelos IPs das interfaces de rede. Em seguida, talvez o mais fundamental, deve-se habilitar o repasse de pacote entre redes, opção sem a qual a máquina não permitirá qualquer atividade de repasse de pacotes, impedindo o funcionamento como *firewall*.

Por fim, habilita-se a entrada e repasse de pacotes de conexões já estabelecidas ou relacionadas a alguma outra regra previamente liberada.

Estas regras são realizadas nas funções REGRAS_BASICAS_FIREWALL e HABILITANDO_NAT do Apêndice B.

4.2 Recursos de PAT

O `Iptables` não tem uma tabela PAT, porém este recurso é suportado na tabela NAT.

A utilização do PAT é sugerida devido a utilização do `Squid` como ferramenta de *proxy* transparente no ambiente desta proposta. O Apêndice B demonstra a utilização do PAT para redirecionar todo o tráfego da porta 80 para a porta 3128, porta então utilizada pelo `Squid`. Esta regra é implementada na função denominada PROXY_TRANSPARENTE.

Foi criado também um *script* complementar (Apêndice C), o qual contém regras para redirecionamento de outros possíveis serviços necessários à realidade da empresa. O Apêndice C demonstra a configuração de PAT para um *desktop* remoto que é muito utilizado para manutenção de sistemas terceirizados.

4.3 Recursos de bloqueio para rede externa

Sugere-se preparar regras para bloqueio de acesso à rede externa,

partindo-se de determinadas máquinas da rede interna. Este recurso pode funcionar como um reforço de segurança da informação para um possível servidor de dados interno, o qual também tem seus controles de acesso habilitados.

O Apêndice B apresenta uma função denominada BLOQUEIO_DE_ACESSO_A_INTERNET com um modelo de implementação de regra.

4.4 Recursos de exceção às regras

Convém estabelecer regras que permitam exceção às regras do firewall para um determinadas máquinas. Este grupo é conhecido tecnicamente como zona desmilitarizada. É um recurso interessante para máquinas administrativas ou áreas específicas de acordo com o ambiente empresarial.

O Apêndice B apresenta uma função denominada GENTE_FINA com um modelo de implementação de regra.

4.5 Implementação da camada sete

Alguns serviços como o MSN entre outros, utiliza vários servidores e portas aleatórios, dificultando o bloqueio de uso através dos recursos normais, ou seja, através do bloqueio tradicional realizado na camada IP. Assim, é sugerido fortemente a implementação de controle na camada sete do modelo OSI ou camada de aplicação no modelo TCP/IP. Para isso, é indicada a ferramenta L7-Filter, que pode bloquear inclusive outros serviços como Yahoo

Messenger, Jabber, entre outros serviços (L7-FILTER, 2008).

O Apêndice B por padrão trás um bloqueio do MSN em especial, sendo a liberação feita através da função denominada LIBERANDO_MSN.

4.6 Liberação de portas para repasse

Deve-se estabelecer regras para liberação apenas das portas necessárias ao funcionamento dos serviços que a empresa necessita. Nesta etapa deve-se descrever as portas redirecionadas quando houver. Este recurso possibilita um melhor controle da máquina *firewall*, intensificando a segurança da própria rede interna.

O Apêndice B apresenta uma função denominada LIBERANDO_PORTAS com um modelo de implementação de regra.

4.7 Definição de ping

Convém estabelecer nas regras de *firewall*, as instruções referente ao tratamento de pacotes *icmp*. Por questões de segurança, este recurso deve ser totalmente bloqueado, dificultando a possibilidade de coleta de informações do servidor.

O Apêndice B por padrão permite ping a partir da rede interna, porém o tratamento de ping a partir de origem externa, é tratado na função denominada DEFININDO_PING como um modelo de implementação.

4.8 Proteção contra formas de ataque comuns

Todo ambiente de rede incluindo a máquina *firewall* estão sujeitos aos mais diversos tipos de ataque que surgem a cada dia, desta forma, deve-se estabelecer uma sessão específica com regras que inibam pelo menos os tipos de ataque mais comuns já conhecidos.

O Apêndice B contém uma função denominada `PROTECAO_CONTRA_ATAQUES`, a qual contém algumas regras para formas de ataque comuns. Nesta função pode-se incluir regras de defesa para outros possíveis ataques comuns.

4.9 Definição de portas utilizadas

Convém estabelecer uma sessão específica para definição das portas a serem utilizadas pelos serviços que a máquina provê. Esta sessão trabalha em conjunto com a sessão de liberação de portas, devendo haver compatibilidade entre ambas, ou seja, não se pode bloquear uma porta que será utilizada por um serviço.

O Apêndice B apresenta uma função denominada `DEFININDO_SSH` com um modelo de implementação de regra, onde a porta padrão do `SSH` é alterada.

4.10 Recursos de NAT

O NAT, recurso essencial a esta proposta, pode ser feito através do

Iptables utilizando a opção MASQUERADE ou SNAT. A diferença entre ambos é que o SNAT permite uma velocidade maior de processamento, pelo fato de que o IP de origem pode ser informado na própria regra. Utilizando o MASQUERADE deverá acontecer um processamento à mais, pois será feita a verificação do IP cada vez que o pacote passa por esta regra. A Figura 19 demonstra uma situação de comparação de ambas as opções.

No Apêndice B, foi utilizada a opção MASQUERADE, pois como uma das conexões externas pode ser ADSL, conseqüentemente não manterá IP fixo.

```
# indicado para IP estatico
iptables -t nat -A POSTROUTING -s 192.168.100.0/24 -o eth0 -j
SNAT -to-source 50.0.0.3

# indicado para IP dinamico
iptables -t nat -A POSTROUTING -s 192.168.100.0/24 -o ppp0 -j
MASQUERADE
```

Figura 19: utilização comparativa de SNAT e MASQUERADE

4.11 Segregação de rede

A segregação de rede deve ser realizada de acordo com a quantidade de máquinas e serviços. Para pequenas empresas, uma única sub-rede classe C pode comportar os usuários e serviços existentes. Em se falando de grandes organizações, este documento propõe que sejam incluídos *firewall* secundários como roteadores na mesma sub-rede da máquina *firewall*. As máquinas de usuários, devem pertencer somente às sub-redes dos respectivos equipamentos de *firewall* e roteamento secundários.

Esta sugestão, além de organizar adequadamente o ambiente de rede

conforme o ítem A.11.4.5 “Segregação de redes” (Fig. 20), provê uma camada maior de segurança.

4.12 Demais regras inerentes à realidade da empresa

A título de complemento do firewall, convém estabelecer uma sessão com regras especiais para serviços de terceiros utilizado pela empresa, desde que não perturbe as demais regras e procedimentos de segurança já estabelecidos.

O Apêndice B demonstra dois casos deste tipo de regras. O primeiro está na função denominada `CONNECTIVIDADE_SOCIAL` e `CONNECTIVIDADE_SOCIAL_NAT`, destinadas a implementação de regras específicas para o serviço de Conectividade Social, da Caixa Econômica Federal, o qual é muito utilizado por grandes empresas. O segundo está na função `DIOPS` e `DIOPS_NAT`, destinadas a implementação de regras específicas para o serviço de DIOPS da Agência Nacional de Saúde.

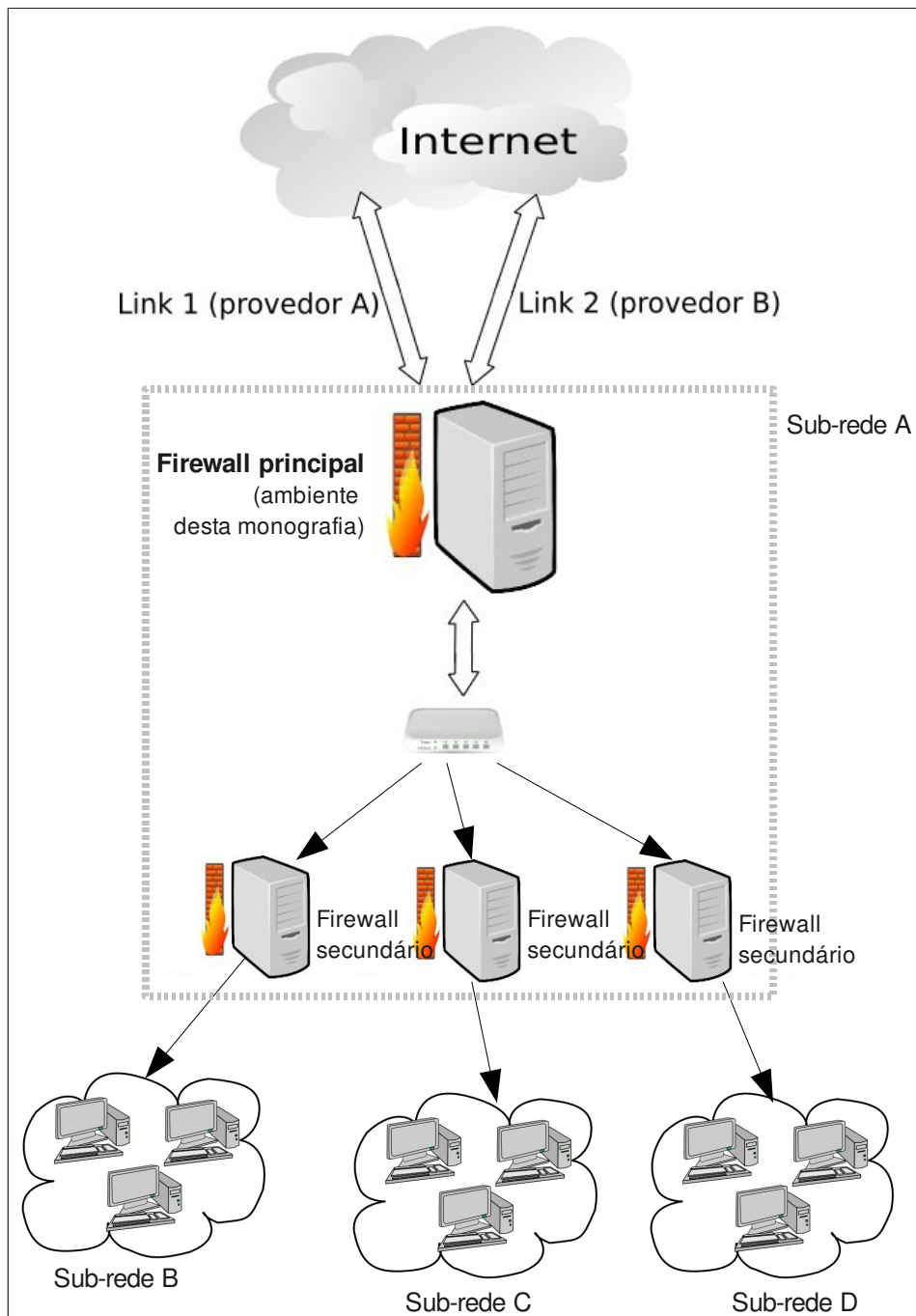


Figura 20: modelo de segregação de rede em ambiente com muitos serviços ou usuários

Capítulo 5

Balanceamento de Carga

Para que o balanceamento de carga ocorra com sucesso, sugere-se a divisão do processo de balanceamento em três partes. A primeira parte refere-se ao processo de detecção das conexões disponíveis. O próximo passo é a ativação do balanceamento através da implementação de tabelas e regras. Por fim vem o último passo, que é a verificação continuada do balanceamento.

5.1. Detecção de conexões e regras existentes

O Apêndice D foi criado com a finalidade de verificar se as conexões estão ativas e as regras de balanceamento existem. Em caso negativo para alguma destas verificações, acontece um tratamento específico para cada caso.

Na verificação de conexões, são testadas as interfaces externas, bem como os respectivos *gateway* de cada *link* externo. Uma vez que todos as conexões externas estejam plenamente habilitadas, passa-se para a verificação de regras de balanceamento, ativando-as se necessário através do Apêndice A.

Quando é detectado que uma das conexões externas está inoperante, o *script* limpa as regras de roteamento e direciona todo o tráfego apenas para o *link* que estiver ativo.

5.2. Balanceamento entre as conexões de internet

Assumindo-se que as conexões estejam plenamente habilitadas, passa-se para a etapa de implementação do balanceamento.

O Apêndice A foi criado especificamente para implementar o que é necessário para estabelecer o balanceamento: arquivo `rt_tables`, rotas nas tabelas auxiliares, rotas na tabela principal, regras de prioridade de roteamento e a regra de balanceamento na tabela principal.

5.2.1 Arquivo `rt_tables`

O balanceamento aqui proposto, requer três tabelas, onde duas delas são específicas para as regras de roteamento dos os *link* externos, sendo uma tabela para cada link. Estas tabelas podem ser utilizadas caso o balanceamento venha a falhar, assumindo todo tráfego para a tabela do *link* que ainda permanece ativo.

A terceira tabela é então reservada para as regras de roteamento balanceado. Convém que a tabela principal seja utilizada para tal finalidade, assim é necessário informar apenas as duas tabelas auxiliares, no `rt_table`. A figura 21 demonstra esta situação, assumindo como auxiliares as tabelas denominadas “velox” e “radio”.

5.2.2. Rotas nas tabelas auxiliares

Cada tabela auxiliar deve receber todas as rotas necessárias a ponto de a tabela funcionar sozinha, sem auxílio de outras tabelas. Isso acontece pelo fato

da possibilidade de falha de rotas definidas em outra tabela ou mesmo na principal. Assim, deve-se estabelecer a rota para o *link* externo e para a rede interna, bem como definir o *gateway* padrão na tabela. A Figura 22 demonstra a saída do comando `ip show table` para a tabela `velox`, com uma descrição das linhas exibidas.

```
#arquivo recriado automaticamente pelo script de roteamento
balanceado
255 local
254 main
253 default

200 velox
201 radio

0 unspec
```

Figura 21: arquivo `rt_tables` recriado com duas tabelas auxiliares

Linha	Saída
1	200.222.117.90 dev ppp0 scope link src 189.12.204.17
2	192.168.100.0/24 dev eth1 scope link src 192.168.100.1
3	default via 200.222.117.90 dev ppp0
Descrição das linhas: 1 – rota para o link externo (usando interface ppp0) 2 – rota para a rede interna (usando interface eth1) 3 – rota para o gateway	

Figura 22: saída do comando `ip show table velox` e descrição de resultado

5.2.3 Rotas na tabela principal

Na tabela principal são definidas as regras de roteamento para os *link* externos e rede interna, além da regra crucial para o balanceamento, que é feita na definição do *gateway*.

A definição do gateway é feito através do recurso de *nexthop* do *iproute*, que tem por finalidade distribuir os pacotes entre os *gateway* externos. Na Figura 23, é demonstrada a saída do comando `ip route show table main`, onde foi definido através do recurso de *nexthop* o balanceamento entre dois *gateway* externos.

```
200.222.117.90 dev ppp0 proto kernel scope link src 189.13.204.17
189.53.151.16/28 dev eth3 proto kernel scope link src 189.53.151.19
192.168.100.0/24 dev eth1 proto kernel scope link src 192.168.100.1
default
    nexthop via 200.222.117.90 dev ppp0 weight 1
    nexthop via 189.43.151.17 dev eth3 weight 1
```

Figura 23: saída do comando `ip route show table main`

5.2.4 Regras de roteamento

A última etapa do balanceamento, é definir as regras de prioridade de uso das tabelas de roteamento. A Figura 24 é um exemplo de saída do comando `ip rule` que tem por objetivo mostrar as regras criadas.

Neste exemplo, foi definido que o tráfego que chega do IP 189.12.204.17 deve seguir as regras da tabela “velox”, e o tráfego do IP 196.13.151.20 deve seguir as regras da tabela “radio”. Em seguida, vem a definição de que tudo deve

verificar a tabela *main* a qual contém as regras de balanceamento. É importante lembrar que a prioridade maior tem valor “0” e a menor “32.767”.

Esta forma de disposição e prioridade dispostas, fazem com que não haja confusão no tráfego que chega, e obriga o balanceamento para o tráfego que sai.

```
0:      from all lookup 255
10000:  from 189.12.204.17 lookup velox
10001:  from 196.13.151.20 lookup radio
32766:  from all lookup main
32767:  from all lookup default
```

Figura 24: saída do comando `ip rule`

5.2.5 Verificação continuada do balanceamento

Quando uma das conexão externas vem a falhar, pode acontecer que a regra de balanceamento seja eliminada automaticamente da tabela principal, parando totalmente a conexão, ficando sem um *gateway* definido. Quando não acontece a eliminação da regra, o balanceamento não funciona de forma adequada. Os pacotes direcionados para este *link* ficarão parados até que o mesmo seja estabelecido novamente.

Essa falha que é prevista e não tem suporte no pacote `iproute`, pode ser resolvida através de uma verificação automatizada em espaços de tempo curtos. O Apêndice D descrito anteriormente realiza esta tarefa. Assim, sugere-se um agendamento de execução deste *script* a cada cinco minutos (Figura 25). O *script* refaz as tabelas, rotas e regras necessárias para a situação em que o ambiente se encontra, habilitando um ou outro *link* ou então o balanceamento se

ambos estão ativos, além ainda de registrar os resultados no arquivo `/var/log/messages` (Figura 26).

```
*/5 * * * * /root/analisa-rede.sh
```

Figura 25: agendamento do Apêndice D através do cron

```
Qua Ago 6 08:50:01 BRT 2008 | Verificacao do link1: ppp0 com GW  
200.222.117.90 | status de erro: 0  
Qua Ago 6 08:50:01 BRT 2008 | Verificacao do link2: eth3 com GW  
189.43.151.17 | status de erro: 0  
Qua Ago 6 08:50:01 BRT 2008 | Verificacao de rota balanceada  
entre 200.222.117.90 e 189.12.204.17 | status de erro: 0
```

Figura 26: trecho do `/var/log/message` com resultados de execução do Apêndice D

Capítulo 6

Resultados obtidos

Em ambos os casos houveram resultados satisfatórios referente à implementação dos controles sugeridos por esta monografia.

A implementação dos controles permitiu um melhoramento significativo na segurança física do ambiente, quesito que anteriormente não era tratado.

O estabelecimento de usuários proprietários bem como o gerenciamento de acesso e gestão de ativos entre outros itens, permitiram uma maior participação na responsabilidades de segurança dos equipamentos e informações por parte dos administradores de sistema.

Os procedimentos de administração remota já eram feitos através de conexão criptografada, porém passaram a ter um monitoramento constante através de arquivos de log.

A segurança dos arquivos do próprio sistema operacional passou a ter uma maior atenção através de controle de integridade de arquivos, controle contra códigos maliciosos e uma conduta de responsabilidade de usuários.

Por fim foi estabelecido o documento política de segurança, com instruções de uso correto dos equipamentos, dicas de formulação de senhas, descrição de itens de controle implementados bem como cláusulas penais referente a possível violação das regras da política.

As regras de *firewall* implementadas, possibilitaram uma filtragem eficiente de pacotes, bloqueando vários serviços anteriormente liberados e que

não eram de interesse da empresa. Também foi reforçado a segurança das portas da máquina *firewall*, fechando o que não é utilizado e alterando a porta padrão para serviços críticos como servidor ssh.

As implementações realizadas, tornaram a máquina *firewall* teoricamente mais segura, porém é necessário um teste de penetração afim de comprovar de forma prática estas implementações.

6.1. Resultados obtidos no caso A

O caso A obteve além dos resultados descritos anteriormente, uma significativa melhoria de aproveitamento de conexões externas de internet através da implementação do balanceamento de carga. Foi possível estabelecer de forma automática, o roteamento do tráfego para as duas conexões externas existentes. Este procedimento permitiu a utilização simultânea das conexões externas, eliminando ociosidade de um dos *link*, bem como a eliminação de necessidade de interferência humana caso uma das conexões venha a falhar.

6.2. Resultados obtidos no caso B

O caso B obteve além dos resultados descritos anteriormente, uma melhoria significativa no monitoramento das conexões existentes, bem como a geração de relatório de acessos. A utilização de monitoração foi essencial para o ambiente, onde a grande maioria das máquinas são destinadas a estudantes em salas de aula e laboratórios, sendo assim necessário um certo controle de

conteúdos acessados.

Dentre os controles descritos, o que gerou maior impacto foi a implementação das regras de *firewall*, pelo fato de permitir um controle na própria instituição sobre as regras de bloqueio bem como os serviços e sites acessados.

Capítulo 7

Conclusão

A implementação sugerida nesta monografia, permitiu ao ambiente computacional estabelecer conformidade com uma norma internacional, melhorando teoricamente a segurança do sistema. Esta teoria pode tornar-se prática através de um procedimento de teste dos controles, validando efetivamente as implementações realizadas, porém este é um possível trabalho futuro.

7.1 Proposta de trabalhos futuros

Esta monografia abre várias possibilidades de trabalhos futuros. Uma proposta de *hardening* para o nível de *kernel* de uma máquina *firewall* é uma potencial proposta de trabalho futuro, podendo ser embasada nesta monografia como ponto inicial. Para tanto é fortemente indicado o uso do `SELinux`.

Uma segunda proposta é a implementação de um teste de penetração a ser realizado após a implementação dos controles descritos nesta monografia. Este funcionaria como uma segunda etapa para o procedimento de *hardening* aqui proposto.

8. REFERÊNCIAS BIBLIOGRÁFICAS

[ABNT, 2008] – Associação Brasileira de Normas Técnicas, disponível em <<https://www.abntnet.com.br/e-commerce/ssl/pesquisaresultado.aspx>>, consulta pelo termo “2700”, acessado em 14/07/2008.

[DEBIAN, 2008] - DEBIAN <<http://www.debian.org>>, acessado em 24/04/2008.

[DOMINGUES, 2003] DOMINGUES, MARCOS AURÉLIO, Comparação de Ferramentas de Verificação de Integridade de Arquivos, Monografia UFLA, 2003.

[FERREIRA, 2003] – FERREIRA, RUBEM E., Linux Guia do Administrador do Sistema, Editora NOVATEC, 2003.

[FREITAS, 2002] – FREITAS, ALLAN EDGARD SILVA – RNP – Rede Nacional de Ensino e Pesquisa, 2002, Disponível em: <http://www.rnp.br/newsgen/0201/roteamento_linux.html>, acessado em 20/02/2008.

[ISO 27001, 2006] – ABNT ISO27001, ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, Tecnologia da Informação – Técnicas de Segurança – Sistemas de gestão de segurança da informação – Requisitos, 2006.

[ISO, 2008] International Organization for Standardization, disponível em <>

acessado em 25/07/2008, procurando pelo termo “27001”, 2008.

[KNOWLEDGELEADER, 2003] Knowledge Leader, disponível em <<http://www.knowledgeleader.com/KnowledgeLeader/Content.nsf/Web+Content/ChecklistsGuidesBritishStandard7799!OpenDocument>>, acessado em 25/07/2008, 2003.

[L7-FILTER, 2008] – APPLICATION LAYER PACKET CLASSIFIER FOR LINUX, atualizado em 23 de abril de 2008 <<http://l7-filter.sourceforge.net/>>, acessado em 26/04/2008.

[LOUREIRO, 2004] – LOUREIRO, HELIO ALEXANDRE LOPES, Ericsson, - Grupo de Trabalho de Engenharia e Operação de Redes - Roteamento Avançado e Controle de Banda em Linux, disponível em <<http://eng.registro.br/gter17/videos/>>, acessado em 20/02/2008 as 9:32am.

[MELO, 2006] – MELO, SANDRO; DOMINGOS, CESAR; CORREIA, LUCAS; MARUYAMA, TIAGO; BS7799 Da tática à prática em servidores linux, Alta Books, 2006.

[MITRE, 2008] - MITRE CORPORATION, Baseline of Guide to the Secure Configuration of Red Hat Enterprise Linux 5, disponível em <<http://cce.mitre.org/lists/data/downloads/cce-rhel5-5.20080305.xls>>, acessado em 15/07/2008.

[NETFILTER, 2008] Netfilter – firewalling, NAT and packet mangling for linux,, disponível em <<http://www.netfilter.org>> acessado em 19/08/2008, 2008.

[NSA, 2008] - National Security Agency – United States of America, Guide to the Secure Configuration of Red Hat Enterprise Linux 5, disponível em <<http://www.nsa.gov/snac/os/redhat/rhel5-guide-i731.pdf>>, acessado em 15/07/2008.

[PALU, 2005] – PALU, ARI JUNIOR, Interface Administrativa para Firewall de Internet em Ambiente Linux, Monografia UFLA, 2005.

[SALTZER, 1975] – SALTZER, JEROME H.; SCHROEDER, MICHAEL D., The Protection of Information in Computer Systems, University of Virginia, disponível em <<http://www.cs.virginia.edu/~evans/cs551/saltzer/>> acessado em 15/07/2008.

[STANDARDS, 2005] Standarts Direct – International Standards And Documentation, disponível em <<http://17799.standardsdirect.org/bs7799.htm>> acessado em 25/07/2008, 2005.

[TEIXEIRA, 2005] – TEIXEIRA, ATALIBA DE O., Uma visão forense dos RootKits em Sistemas Linux, Monografia UFLA, 2005.

[TLDP, 2000] - THE LINUX DOCUMENTATION PROJECT, Firewall and Proxy Server HOWTO, Mark Grennan, <<http://tldp.org/HOWTO/Firewall-HOWTO-2.html#ss2.2>>, acessado em 24/04/2008.

APÊNDICES

APÊNDICE A – arquivo balanceamento.sh

```
#!/bin/bash
#-----
# arquivo : balanceamento.sh
# objetivo : criar tabelas de roteamento balanceado
# obs. : as interfaces de rede ja devem estar previamente
#        configuradas
# autor : Dorival M Machado Junior(dorivaljunior@gmail.com)
#-----
# PREENCHIMENTO DE VARIAVEIS

# comandos utilizados
IFCONFIG="/sbin/ifconfig"
SED="/bin/sed"
AWK="/usr/bin/awk"
IP="/sbin/ip"
GREP="/bin/grep"

# interface externa 1 (utilizando velox)
IF1="ppp0"
IP1=$( $IFCONFIG $IF1 | $SED s/end.:/addr:/ | $AWK '/inet
addr:/' | $SED 's/.*addr:/' | $AWK {'print $1'} )
P1=$( $IFCONFIG $IF1 | $AWK '/P-a-P:/' | $SED 's/.*P-a-P:/' |
$AWK {'print $1'} ) # gateway
P1_NET="200.2.117.90/32"

# interface externa 2 (utilizando internet via rádio)
IF2="eth3"
IP2=$( $IFCONFIG $IF2 | $SED s/end.:/addr:/ | $AWK '/inet
addr:/' | $SED 's/.*addr:/' | $AWK {'print $1'} )
P2="181.51.171.19"
P2_NET="181.51.171.16/28"

# interface interna
IF1_INTERNA="eth1"
IP1_INTERNA=$( $IFCONFIG $IF1_INTERNA | $SED s/end.:/addr:/ |
$AWK '/inet addr:/' | $SED 's/.*addr:/' | $AWK {'print $1'} )
P1_NET_INTERNA="192.168.100.0/24"

# configuracao das tabelas de roteamento
RT_TABLES="/etc/iproute2/rt_tables"
TABELA1="velox"
PRIORIDADE_TABELA1="10000"
TABELA2="radio"
PRIORIDADE_TABELA2="10001"

#----- FIM DO PREENCHIMENTO DE VARIAVEIS-----
echo "Configurando o roteamento."
echo "Recriando o arquivo $RT_TABLES."
echo "#arquivo recriado automaticamente pelo script de
```

```

roteamento balanceado" > $RT_TABLES
echo "255 local" >> $RT_TABLES
echo "254 main" >> $RT_TABLES
echo "253 default" >> $RT_TABLES
echo "" >> $RT_TABLES
echo "200 $TABELA1" >> $RT_TABLES
echo "201 $TABELA2" >> $RT_TABLES
echo "" >> $RT_TABLES
echo "0 unspec" >> $RT_TABLES

echo "Adicionando rotas para redes externas nas tabelas $TABELA1
e $TABELA2"
$IP route add $P1_NET dev $IF1 src $IP1 table $TABELA1 >
/dev/null 2>&1
$IP route add default via $P1 table $TABELA1 > /dev/null 2>&1
$IP route add $P2_NET dev $IF2 src $IP2 table $TABELA2 >
/dev/null 2>&1
$IP route add default via $P2 table $TABELA2 > /dev/null 2>&1

echo "Adicionando rotas para rede interna nas tabelas $TABELA1
e $TABELA2"
$IP route add $P1_NET_INTERNA dev $IF1_INTERNA src $IP1_INTERNA
table $TABELA1 > /dev/null 2>&1
$IP route add $P1_NET_INTERNA dev $IF1_INTERNA src $IP1_INTERNA
table $TABELA2 > /dev/null 2>&1

echo "Adicionando rotas na tabela principal"
$IP route add $P1_NET dev $IF1 src $IP1 > /dev/null 2>&1
$IP route add $P2_NET dev $IF2 src $IP2 > /dev/null 2>&1

echo "Adicionando regras de roteamento para tabelas $TABELA1 e
$TABELA2"
ROTA_IP1=$( $IP rule | $GREP $IP1)
ROTA_IP2=$( $IP rule | $GREP $IP2)

if [ -z "$ROTA_IP1" ]
then
    $IP rule add prio $PRIORIDADE_TABELA1 from $IP1 table
$TABELA1
fi

if [ -z "$ROTA_IP2" ]
then
    $IP rule add prio $PRIORIDADE_TABELA2 from $IP2 table
$TABELA2
fi

echo "Adicionando regra de roteamento balanceado"
$IP route del default # 2>&1
$IP route add default scope global nexthop via $P1 dev $IF1
weight 2 nexthop via $P2 dev $IF2 weight 1 > /dev/null 2>&1

```

APENDICE B - arquivo mirar-firewall-dorival.sh

```
#!/bin/bash
#-----
# MIRAR Firewall - script de firewall
# arquivo   : mirar-firewall-dorival.sh
# objetivo  : execução de regras de firewall
# autor     : Dorival M Machado Junior(dorivaljunior@gmail.com)
# versao    : 5.05, em 2 de julho de 2008
#-----

LEITURA_DE_VARIAVEIS()
{
    # ----- preenchimento de variaveis -----

    # LOCALIZACAO DOS COMANDOS NECESSARIOS
    # -----

    IPTABLES="/sbin/iptables"
    IFCONFIG="/sbin/ifconfig"

    # CONFIGURACAO DA REDE
    # -----

    # configuracao da placa interna.
    LAN_INTERNA1="eth0:2"

    LANS_INTERNAS="eth0:2"

    # rede(s) interna(s) permitida(s) para acesso a internet.
    MINHA_REDE="100.100.100.0/24"

    # configuracao da placa externa 1.
    LAN_EXTERNAL1="eth0"

    # configuracao da placa externa 2
    LAN_EXTERNAL2="eth0:1"

    LANS_EXTERNAS="eth0 eth0:1"

    # IP externo 1
    IP_EXTERNO1=$(($IFCONFIG $LAN_EXTERNAL1 | sed s/end.:/addr:/
| awk '/inet addr:/' | sed 's/.*addr:/' | awk {'print $1'} )

    # IP externo 2
    IP_EXTERNO2=$(($IFCONFIG $LAN_EXTERNAL2 | sed
s/end.:/addr:/ | awk '/inet addr:/' | sed 's/.*addr:/' | awk
{'print $1'} )
```

```

IPS_EXTERNOS="$IP_EXTERNO1 $IP_EXTERNO2"

# IP interno
IP_INTERNO1=$(IFSCONFIG      $LAN_INTERNA1      |      sed
s/end.:/addr:/ | awk '/inet addr:/' | sed 's/.*addr:/' | awk
{'print $1'} )

# OPCOES DE CONFIGURACAO DO FIREWALL
# -----

# Porta SSH (padrao = 22)
PORTA_SSH="63695"

# Portas altas
PORTAS_ALTAS="1024:65535"

# Utiliza proxy transparente ? (y=sim n=nao)
# obs.: o squid ja deve estar rodando
TRANSPARENTE="n"

# Permissao de ping para o IP externo
# (IP interno recebe ping por padrao)
PING="y"

# ARQUIVOS AUXILIARES
# -----
# os arquivos auxiliares devem conter um valor (IP ou
porta) por linha

# Lista de maquinas liberadas para usar MSN
ARQUIVO_LIBERA_MSN="/etc/mirar-firewall/libera_msn.txt"
LIBERA_MSN=$( cat $ARQUIVO_LIBERA_MSN | grep -v ^# |
grep . )

# Portas a serem bloqueadas para repasse a rede externa
ARQUIVO_PORTAS_BLOQUEADAS="/etc/mirar-
firewall/blocked_door.txt"
PORTAS_BLOQUEADAS=$( cat $ARQUIVO_PORTAS_BLOQUEADAS | grep
-v ^# | grep . )

# Portas a serem liberadas para repasse a rede externa
ARQUIVO_PORTAS_LIBERADAS="/etc/mirar-
firewall/open_door.txt"
PORTAS_LIBERADAS=$( cat $ARQUIVO_PORTAS_LIBERADAS | grep -
v ^# | grep . )

# IPs externos que serao totalmente bloqueados
IP_BLOQUEADO="/etc/mirar-firewall/blocked_ip.txt"
SITES_BLOQUEADOS=$( cat $IP_BLOQUEADO | grep -v ^# |

```

```

grep . )

# Maquinas que serao excessao aos bloqueios de IP e portas
FINE_PEOPLE="/etc/mirar-firewall/fine_people.txt"
GENTE_FINA=$( cat $FINE_PEOPLE | grep -v ^# | grep . )

# Regras de redirecionamentos de trafego (ex.: VNC)
SCRIPT_REDIRECT="/etc/mirar-firewall/redirect.sh"

# Lista de IPs internos bloqueados para uso de internet
NO_INTERNET="/etc/mirar-firewall/no_internet.txt"
SEM_INTERNET=$( cat $NO_INTERNET | grep -v ^# |\ grep . )

# OPCOES ESPECIAIS
# -----

# Utiliza servico de Conectividade Social da
# Caixa Economica Federal (y=sim n=nao)
CONNECTIVIDADE="y"

# Utiliza servico de DIOPS da Agencia Nacional
# de Saude
DIOPS="y"

# ===== fim do preenchimento de variaveis =====
}

LIMPO()
{
    echo "Definindo todas politicas como ACCEPT"
    $IPTABLES -P INPUT ACCEPT
    $IPTABLES -P OUTPUT ACCEPT
    $IPTABLES -P FORWARD ACCEPT

    echo "Liberando loopback..."
    $IPTABLES -A INPUT -d 127.0.0.1 -j ACCEPT
    $IPTABLES -A OUTPUT -d 127.0.0.1 -j ACCEPT

    for REDE_INTERNA in $MINHA_REDE
    do
        echo "Liberando forward entre a rede
$REDE_INTERNA e Internet."
        $IPTABLES -A FORWARD -s $REDE_INTERNA -d 0/0 -
j ACCEPT
        $IPTABLES -A FORWARD -d $REDE_INTERNA -s 0/0 -
j ACCEPT
    done

    #obs.: a regra de NAT esta numa funcao propria

```

```

}

INICIANDO()
{
    echo -ne '\033[11;200]\033[10;900]\a'
    echo -e '\033[33;1m=====> INICIANDO MIRAR
FIREWALL, BY DORIVAL JUNIOR(dorivaljunior@gmail.com):\033[m'
    echo -e '\033[33m'
}

LIMPANDO_REGRAS()
{
    echo "Limpendo regras existentes..."
    $IPTABLES -F
    $IPTABLES -F -t nat
}

DEFININDO_POLITICAS_PRINCIPAIS()
{
    echo "Definindo politica restritiva..."
    $IPTABLES -P INPUT DROP
    $IPTABLES -P OUTPUT DROP
    $IPTABLES -P FORWARD DROP
}

PARANDO_CONEXOES()
{
    $IPTABLES -P INPUT DROP
    $IPTABLES -P OUTPUT DROP
    $IPTABLES -P FORWARD DROP
}

INFORMACOES()
{
    echo "CONFIGURACAO DE REDE ATUAL:"
    echo "  Interface interna ($LAN_INTERNAL) com IP:
$IP_INTERNO1"
    echo "  Interface externa 1 ($LAN_EXTERNAL1) com IP:
$IP_EXTERNO1"
    echo "  Interface externa 2 ($LAN_EXTERNAL2) com IP:
$IP_EXTERNO2"
}

ESTADO_DE_CONEXAO()
{
    echo "Bloqueando repasse de conexoes invalidas"
    $IPTABLES -A FORWARD -s 0/0 -d 0/0 -m state --state
INVALID -j DROP
}

```



```

        echo "Bloqueando entrada de conexoes invalidas"
        $IPTABLES -A INPUT -s 0/0 -m state --state INVALID -j
DROPO
        echo "Permitindo repasse de pacotes relacionados ou
conexoes estabelecidas"
        $IPTABLES -A FORWARD -s 0/0 -d 0/0 -m state --state
ESTABLISHED,RELATED -j ACCEPT
        echo "Permitindo entrada de pacotes relacionados ou
conexoes estabelecidas"
        $IPTABLES -A INPUT -s 0/0 -m state --state
ESTABLISHED,RELATED -j ACCEPT
    }

REDIRECIONAMENTO_DE_PORTAS()
{
    if [ ! -z "$SCRIPT_REDIRECT" ]
    then
        echo "Executando script de redirecionamento
de trafego especificos para maquinas internas
($SCRIPT_REDIRECT). "
        $SCRIPT_REDIRECT
    fi
}

BLOQUEIO_DE_ACESSO_A_INTERNET()
{
    if [ ! -z "$SEM_INTERNET" ]
    then
        echo "Bloqueio de internet:"
        for NO_NET in $SEM_INTERNET
        do
            echo " Bloqueando o acesso a
internet para o IP: $NO_NET"
            $IPTABLES -A INPUT -s $NO_NET -j DROP
            $IPTABLES -A OUTPUT -s $NO_NET -j DROP
            $IPTABLES -A FORWARD -s $NO_NET -d
0/0 -j DROP
            $IPTABLES -A FORWARD -s 0/0 -d $NO_NET
-j DROP
        done
    fi
}

GENTE_FINA()
{
    if [ ! -z "$GENTE_FINA" ]
    then
        if [ ! -z "$SITES_BLOQUEADOS" ]
        then

```

```

                                echo "Liberação das regras de
bloqueio:"
                                for MAQ_LIB in $GENTE_FINA
                                do
                                    echo "    Liberando o repasse
para qualquer porta e IP originado do IP $MAQ_LIB"
                                    $IPTABLES -A FORWARD -s
$MAQ_LIB -d 0/0 -j ACCEPT
                                    $IPTABLES -A FORWARD -d
$MAQ_LIB -s 0/0 -j ACCEPT
                                done
                                fi
                                fi
                                }

LIBERANDO_MSN()
{
    if [ ! -z "$LIBERA_MSN" ]
    then
        echo "Liberação do MSN:"
        for MSNLIB in $LIBERA_MSN
        do
            echo "    Liberando MSN para o
IP: $MSNLIB (camada 7)"
            $IPTABLES -A FORWARD -s
$MSNLIB -m layer7 --l7proto msnmessenger -j ACCEPT
            $IPTABLES -A FORWARD -s
$MSNLIB -p tcp --dport $PORTA_MSN -j ACCEPT
            done
        fi
    }

LIBERANDO_PORTAS()
{
    if [ ! -z "$PORTAS_LIBERADAS" ]
    then
        echo "Liberação de portas:"
        for LIBERAPORTA in $PORTAS_LIBERADAS
        do
            for REDE_INTERNA in $MINHA_REDE
            do
                echo "    Liberando repasse
TCP/UDP da rede local($REDE_INTERNA) pela porta $LIBERAPORTA."
                $IPTABLES -A FORWARD -s
$REDE_INTERNA -p tcp -d 0/0 --dport $LIBERAPORTA -j ACCEPT
                $IPTABLES -A FORWARD -s
$REDE_INTERNA -p udp -d 0/0 --dport $LIBERAPORTA -j ACCEPT
            done
        done
    }
}

```

```

done
done
fi
}

BLOQUEIO_DE_PORTAS()
{
    if [ ! -z "$PORTAS_BLOQUEADAS" ]
    then
        echo "Bloqueio de portas proibidas:"
        for PORTA in $PORTAS_BLOQUEADAS
        do
            for REDE_INTERNA in $MINHA_REDE
            do
                echo " Bloqueando repasse
TCP/UDP da rede local($REDE_INTERNA) pela porta $PORTA"
                $IPTABLES -A FORWARD -s
$REDE_INTERNA -p tcp --dport $PORTA -j DROP
                $IPTABLES -A FORWARD -s
$REDE_INTERNA -p udp --dport $PORTA -j DROP
            done
        done
    fi
}

BLOQUEIO_DE_IPS()
{
    if [ ! -z "$SITES_BLOQUEADOS" ]
    then
        echo "Bloqueio de IPs proibidos:"
        for SITE in $SITES_BLOQUEADOS
        do
            for REDE_INTERNA in $MINHA_REDE
            do
                echo " Bloqueando o IP $SITE
para a rede $REDE_INTERNA."
                $IPTABLES -A FORWARD -s
$REDE_INTERNA -d $SITE -j DROP
                $IPTABLES -A FORWARD -d
$REDE_INTERNA -s $SITE -j DROP
            done
        done
    fi
}

BLOQUEIO_DO_MSN()
{

```

```

        for REDE_INTERNA in $MINHA_REDE
        do
            echo "Bloqueando MSN para a rede $REDE_INTERNA
(camada 7)"
                $IPTABLES -A FORWARD -s $REDE_INTERNA -m
layer7 --l7proto msnmessenger -j DROP
                $IPTABLES -A FORWARD -s $REDE_INTERNA -p tcp
--dport $PORTA_MSN -j DROP
                if [ "$BLOCK_MSN_FILE" = "y" ]
                then
                    echo "Bloqueando a transferencia de
arquivos do MSN (camada 7) - (EXPERIMENTAL)"
                    $IPTABLES -A FORWARD -s $REDE_INTERNA
-m layer7 --l7proto msn-filetransfer -j DROP
                fi
                done
        }

REGRAS_BASICAS_FIREWALL()
{
    # REGRAS BASICAS DO GATEWAY (DEVE VIR APOS DEFINICAO
DE BLOQUEIOS DE INPUT E FORWARD DA REDE INTERNA)

    # LIBERANDO LOOPBACK
    echo "Liberando loopback..."
    $IPTABLES -A INPUT -d 127.0.0.1 -j ACCEPT
    $IPTABLES -A OUTPUT -d 127.0.0.1 -j ACCEPT

    for REDE_INTERNA in $MINHA_REDE
    do
        echo "Liberando INPUT originado da rede
$REDE_INTERNA"
            $IPTABLES -A INPUT -s $REDE_INTERNA -j ACCEPT

            echo "Liberando forward entre a rede
$REDE_INTERNA e Internet."
            $IPTABLES -A FORWARD -s $REDE_INTERNA -d 0/0 -
j ACCEPT
            $IPTABLES -A FORWARD -d $REDE_INTERNA -s 0/0 -
j ACCEPT
            done
    }

DEFININDO_PING()
{
    if [ "$PING" = "y" ]
    then
        ACAO="ACCEPT"
        PINGFOI="LIBERADO"
    fi
}

```

```

else
    ACAA="REJECT"
    PINGFOI="BLOQUEADO"
fi

for EXTERNOS_IPS in $IPS_EXTERNOS
do
    echo "O ping para o IP $EXTERNOS_IPS foi
$PINGFOI"
    for TIPO in 0 3 8 11
    do
        $IPTABLES -A INPUT -p icmp -s 0/0 -d
$EXTERNOS_IPS --icmp-type $TIPO -j $ACAO
        $IPTABLES -A OUTPUT -p icmp -s
$EXTERNOS_IPS -d 0/0 --icmp-type $TIPO -j $ACAO
    done
done
}

PROTECAO_CONTRA_ATAQUES()
{
    echo "Aplicando proteção contra Syn-flood e DOS"
    $IPTABLES -A FORWARD -p tcp --syn -m limit --limit 1/s
-j ACCEPT

    echo "Aplicando proteção contra scanners de porta"
    $IPTABLES -A FORWARD -p tcp --tcp-flags
SYN,ACK,FIN,RST RST -m limit --limit 1/s -j ACCEPT
    $IPTABLES -A FORWARD -p tcp --tcp-flags ALL SYN,ACK -j
DROP
}

DEFININDO_SSH()
{
    for EXTERNOS_IPS in $IPS_EXTERNOS
    do
        echo "Liberando recebimento de SSH pela porta
$PORTA_SSH no IP $EXTERNOS_IPS"
        $IPTABLES -A INPUT -p tcp -s 0/0 --sport
$PORTAS_ALTAS -d $EXTERNOS_IPS --dport $PORTA_SSH -j ACCEPT
    done
}

CONECTIVIDADE_SOCIAL()
{
    if [ "$CONECTIVIDADE" = "y" ]
    then
        for REDE_INTERNA in $MINHA_REDE
        do

```

```

                                echo "CONECTIVIDADE SOCIAL: Liberando
repassse TCP de $REDE_INTERNA para portas e IPs especificos"
                                $IPTABLES -A FORWARD -s $REDE_INTERNA
-p tcp -d 200.201.174.207 --dport 80 -j ACCEPT
                                $IPTABLES -A FORWARD -s $REDE_INTERNA
-p tcp -d 200.201.174.204 --dport 80 -j ACCEPT
                                $IPTABLES -A FORWARD -s $REDE_INTERNA
-p tcp -d 200.201.174.204 --dport 2631 -j ACCEPT
                                $IPTABLES -A FORWARD -p tcp -d
200.201.0.0/16 -j ACCEPT
                                done
                                fi
                                }

DIOPS_ANS()
{
    if [ "$DIOPS" = "y" ]
    then
        for REDE_INTERNA in $MINHA_REDE
        do
            echo "DIOPS: Liberando repases TCP de
$REDE_INTERNA para portas e Ips especificos"
            $IPTABLES -t nat -A PREROUTING -p tcp
-d 200.255.42.71 -j ACCEPT
            $IPTABLES -A FORWARD -s $REDE_INTERNA
-p tcp -d 200.255.42.71 --dport 80 -j ACCEPT
            $IPTABLES -A FORWARD -s $REDE_INTERNA
-p tcp -d 200.255.42.71 --dport 21 -j ACCEPT
            $IPTABLES -A FORWARD -s $REDE_INTERNA
-p tcp -d 200.255.42.71 --dport 20000:20020 -j ACCEPT
            done
            fi
        }

#===== REGRAS ESPECIAIS DE NAT =====

HABILITANDO_NAT()
{
    echo "====> APLICANDO REGRAS NA TABELA NAT"
    echo "Ativando repasse entre redes no
/proc/sys/net/ipv4/ip_forward"
    echo 1 > /proc/sys/net/ipv4/ip_forward

    for REDE_INTERNA in $MINHA_REDE
    do
        for EXTERNAS_LANS in $LANS_EXTERNAS
        do

```

```

                                echo "Fazendo mascaramento entre
$REDE_INTERNA e $EXTERNAS_LANS"
                                $IPTABLES -t nat -A POSTROUTING -s
$REDE_INTERNA -o $EXTERNAS_LANS -j MASQUERADE
                                done
                                done
                                }

CONECTIVIDADE_SOCIAL-NAT()
{
    if [ "$CONECTIVIDADE" = "y" ]
    then
        echo "CONECTIVIDADE SOCIAL: Liberando pre-
roteamento para IPs da Caixa Economica Federal"
        $IPTABLES -t nat -A PREROUTING -p tcp -d
200.201.0.0/16 -j ACCEPT
        fi
    }

DIOPS_ANS-NAT()
{
    if [ "$DIOPS" = "y" ]
    then
        for INTERNAS_LANS in $LANS_INTERNAS
        do
            echo "DIOPS: Liberando pre-roteamento
pelas portas 21 e 20000 a 20019 e IP especifico para\
$INTERNAS_LANS"
            $IPTABLES -t nat -A PREROUTING -i
$INTERNAS_LANS -p tcp --dport 20000:20019 -j ACCEPT
            $IPTABLES -t nat -A PREROUTING -i
$INTERNAS_LANS -p tcp --dport 21 -j ACCEPT
            $IPTABLES -t nat -A PREROUTING -p tcp
-d 200.255.42.71 -j ACCEPT
            done
        fi
    }

PROXY_TRANSPARENTE()
{
    if [ "$TRANSPARENTE" = "y" ]
    then
        if [ ! -z "$NO_PROXY_TRANSP" ]
        then
            for SEM_PROXY in $NO_PROXY_TRANSP
            do
                for INTERNAS_LANS in
$LANS_INTERNAS

```

```

do
    $IPTABLES -t nat -A
PREROUTING -i $INTERNAS_LANS -p tcp -d ! $SEM_PROXY --dport 80 -
j REDIRECT --to-port 3128
    echo "Definindo proxy
transparente para $INTERNAS_LANS com excessao para $SEM_PROXY"
done
done
else
    for INTERNAS_LANS in $LANS_INTERNAS
do
    echo "Definindo proxy
transparente para $INTERNAS_LANS."
    $IPTABLES -t nat -A PREROUTING
-i $INTERNAS_LANS -p tcp --dport 80 -j REDIRECT --to-port 3128
done
fi
fi
}

FINALIZANDO()
{
    echo ""
    echo -e '\033[33;1m===== > REGRAS DE FIREWALL
APLICADAS.\033[m'

    echo -ne '\033[11;100]\033[10;1100]\a'

    echo -ne '\033[11;100]\033[10;750]'
    echo ""
}

AJUDA()
{
    echo "MIRAR Firewall, por Dorival M Machado
Junior(dorivaljunior@gmail.com)"
    echo ""
    echo " Opcoes: apply - executa as regras
normalmente"
    echo " stop - para totalmente o firewall,
bloqueando todas as conexoes"
    echo " clean - executa regras limpas, sem
qualquer tipo de bloqueio"
}

case "$1" in
    stop)
        LEITURA_DE_VARIAVEIS
        LIMPANDO_REGRAS
        PARANDO_CONEXOES

```



```

;;

apply)
    LEITURA_DE_VARIAVEIS
    INICIANDO
    LIMPANDO_REGRAS
    DEFININDO_POLITICAS_PRINCIPAIS
    INFORMACOES
    ESTADO_DE_CONEXAO
    REDIRECIONAMENTO_DE_PORTAS
    BLOQUEIO_DE_ACESSO_A_INTERNET
    GENTE_FINA
    LIBERANDO_MSN
    LIBERANDO_PORTAS
    BLOQUEIO_DE_PORTAS
    BLOQUEIO_DE_IPS
    BLOQUEIO_DO_MSN
    REGRAS_BASICAS_FIREWALL
    DEFININDO_PING
    PROTECAO_CONTRA_ATAQUES
    DEFININDO_SSH
    CONECTIVIDADE_SOCIAL
    DIOPS_ANS
    HABILITANDO_NAT
    CONECTIVIDADE_SOCIAL-NAT
    DIOPS_ANS-NAT
    PROXY_TRANSPARENTE
    FINALIZANDO

;;

clean)
    LEITURA_DE_VARIAVEIS
    INICIANDO
    LIMPANDO_REGRAS
    LIMPO
    INFORMACOES
    HABILITANDO_NAT
    PROXY_TRANSPARENTE
    FINALIZANDO

;;

help)
    AJUDA

;;

*)
echo "Uso: $0 {apply|stop|clean|help}"
;;

esac

```

APENDICE C - arquivo redirect.sh

```
#!/bin/bash
#-----
# MIRAR Firewall
# arquivo : redirect.sh
# objetivo : regras de redirecionamento
# autor   : Dorival M Machado Junior (dorivaljunior@gmail.com)
# versao  : 1.00, em 5 de maio de 2008
#-----

# Regras especiais de redirecionamento

# DESKTOP REMOTO
RDESKTOP="3389"
DESTINO_RDESKTOP="192.168.100.100"
IPT="/sbin/iptables"
#-----
$IPT -t nat -A PREROUTING -p tcp --dport $RDESKTOP -j DNAT
--to-destination $DESTINO_RDESKTOP
$IPT -t nat -A PREROUTING -p udp --dport $RDESKTOP -j DNAT
--to-destination $DESTINO_RDESKTOP
$IPT -t nat -A OUTPUT -p tcp --dport $RDESKTOP -j DNAT --to-
destination $DESTINO_RDESKTOP
$IPT -t nat -A OUTPUT -p udp --dport $RDESKTOP -j DNAT --to-
destination $DESTINO_RDESKTOP
echo " Redirecionando $RDESKTOP para $DESTINO_RDESKTOP"
#-----

#PARA FAZER UM NOVO REDIRECIONAMENTO, BASTA DESCOMENTAR TODAS
AS LINHAS ABAIXO E CONFIGURAR A PORTA E DESTINO
#PORTA=""
#DESTINO=""
#$IPT -t nat -A PREROUTING -p tcp --dport $RDESKTOP -j DNAT --
to-destination $DESTINO_RDESKTOP
#$IPT -t nat -A PREROUTING -p udp --dport $RDESKTOP -j DNAT --
to-destination $DESTINO_RDESKTOP
#$IPT -t nat -A OUTPUT -p tcp --dport $RDESKTOP -j DNAT --to-
destination $DESTINO_RDESKTOP
#$IPT -t nat -A OUTPUT -p udp --dport $RDESKTOP -j DNAT --to-
destination $DESTINO_RDESKTOP
#echo " Redirecionando $PORTA para $DESTINO"
```

APENDICE D - arquivo analisa-rede.sh

```
#!/bin/bash
#-----
# objetivo      : teste de regras de balanceamento e links de
acesso externos
# autor         : Dorival M Machado Junior,
dorivaljunior@gmail.com
# versao        : 1.0
#-----

#Preenchimento de variaveis

#comandos necessarios
SCRIPT_BALANCEAMENTO="/root/balanceamento.sh"
IFCONFIG="/sbin/ifconfig"
CAT="/bin/cat"
PING="/bin/ping"
IP="/sbin/ip"
ARQUIVO_DE_LOG="/var/log/messages"

#informacoes da rede
INTERFACE_LINK1="ppp0"
IP_LINK1=$( $IFCONFIG $INTERFACE_LINK1 | sed s/end.:/addr:/ |
awk /'inet addr:/' | sed 's/.*addr:/' | awk {'print $1'} )
GATEWAY_LINK1=$( $IFCONFIG $INTERFACE_LINK1 | awk /'P-a-P:/' |
sed 's/.*P-a-P:/' | awk {'print $1'} )
INTERFACE_LINK2="eth3"
IP_LINK2="189.43.151.19"
GATEWAY_LINK2="189.43.151.17"

#-----

DATA=$(/bin/date)

VERIFICA_INTERFACE1(){
  TESTE_INTERFACE_LINK1=$( $CAT /proc/net/dev | grep
$INTERFACE_LINK1 )
  if [ ! -z "$TESTE_INTERFACE_LINK1" ]
  then
    LINK1="0"
  else
    LINK1="1"
  fi
}

VERIFICA_INTERFACE2(){
  TESTE_INTERFACE_LINK2=$( $CAT /proc/net/dev | grep
$INTERFACE_LINK2 )
```

```

if [ ! -z "$TESTE_INTERFACE_LINK2" ]
then
    LINK2="0"
else
    LINK2="1"
fi
}

VERIFICA_GW1(){

if ($PING -c 2 $GATEWAY_LINK1 > /dev/null 2>&1)
then
    LINK1="0"
else
    LINK1="1"
fi
}

VERIFICA_GW2(){
if ($PING -c 2 $GATEWAY_LINK2 > /dev/null 2>&1)
then
    LINK2="0"
else
    LINK2="1"
fi
}

VERIFICA_ROTA_BALANCEADA(){
TESTE_ROTA_BALANCEADA=$(($IP route | grep nexthop )
if [ ! -z "$TESTE_ROTA_BALANCEADA" ]
then
    ROTA_BALANCEADA="0"
else
    ROTA_BALANCEADA="1"
fi
}

LIMPA_ROTA_DEFAULT(){
$IP route del default
$IP route del default via $INTERFACE_LINK1 2>&1
$IP route del default via $INTERFACE_LINK2 2>&1
$IP route del default via $GATEWAY_LINK1 2>&1
$IP route del default via $GATEWAY_LINK2 2>&1
$IP route del default via $GATEWAY_LINK1 dev $INTERFACE_LINK1
2>&1
$IP route del default via $GATEWAY_LINK2 dev $INTERFACE_LINK2
2>&1
}

CONFERE_REGRAS(){

```

```

REGRA_GW1=$(ip rule | grep $IP_LINK1)
REGRA_GW2=$(ip rule | grep $IP_LINK2)

if [ -z "$REGRA_GW1" -o -z "$REGRA_GW2" ]
then
    # falta alguma regra
    $SCRIPT_BALANCEAMENTO
    echo "$DATA | Regras de roteamento (ip rule)
inconsistentes, atualizando..." >> $ARQUIVO_DE_LOG
fi

}

#INICIO DA EXECUCAO DE COMANDOS

#verificando se as interfaces estao levantadas
VERIFICA_INTERFACE1
VERIFICA_INTERFACE2

#verificando os gateways caso as interfaces estejam ok
if [ "$LINK1" = "0" ]
then
    VERIFICA_GW1
fi

if [ "$LINK2" = "0" ]
then
    VERIFICA_GW2
fi

#jogando resultado no arquivo de log
echo "$DATA | Verificacao do link1: $INTERFACE_LINK1 com GW
$GATEWAY_LINK1 | status de erro: $LINK1" >> $ARQUIVO_DE_LOG
echo "$DATA | Verificacao do link2: $INTERFACE_LINK2 com GW
$GATEWAY_LINK2 | status de erro: $LINK2" >> $ARQUIVO_DE_LOG

# verificando a rota balanceada caso os links e gateway
estejam ok
VERIFICA_ROTA_BALANCEADA

if [ "$LINK1" = "0" -a "$LINK2" = "0" ]
then
    if [ "$ROTA_BALANCEADA" = "0" ]
    then
        echo "$DATA | Verificacao de rota balanceada entre
$GATEWAY_LINK1 e $GATEWAY_LINK2 | status de erro:
$ROTA_BALANCEADA" >> $ARQUIVO_DE_LOG
        CONFERE_REGRAS
        exit 0
    else
        echo "$DATA | Verificacao da rota balanceada |

```

```

status de erro: $ROTA_BALANCEADA | re-ativando o balanceamento"
>> $ARQUIVO_DE_LOG
    LIMPA_ROTA_DEFAULT
    $SCRIPT_BALANCEAMENTO
    exit 0
fi
else
    #algum link esta inoperante, entao verificar qual e
estabecer a nova rota
    if [ "$LINK1" = "1" -a "$LINK2" = "0" ]
    then
        # comandos para estabelecer rota pelo link2
        LIMPA_ROTA_DEFAULT
        $IP route add default via $GATEWAY_LINK2 dev
$INTERFACE_LINK2
        $IP rule del from $GATEWAY_LINK1 #apagando regra de
uso do gateway 1
        $IP route flush cache
        echo "$DATA | Rota re-estabelecida usando GW
$GATEWAY_LINK2 via $INTERFACE_LINK2" >> $ARQUIVO_DE_LOG
        exit 0
    fi
    if [ "$LINK1" = "0" -a "$LINK2" = "1" ]
    then
        # comandos para estabelecer rota pelo link1
        LIMPA_ROTA_DEFAULT
        $IP route add default via $GATEWAY_LINK1 dev
$INTERFACE_LINK1
        $IP rule del from $GATEWAY_LINK2 #apagando regra de
uso do gateway 1
        $IP route flush cache
        echo "$DATA | Rota re-estabelecida usando GW
$GATEWAY_LINK1 via $INTERFACE_LINK1" >> $ARQUIVO_DE_LOG
        exit 0
    fi
fi
echo "$DATA | Link $INTERFACE_LINK1 e $INTERFACE_LINK2
inoperantes; impossivel estabelecer nova rota" >>
$ARQUIVO_DE_LOG

```

APENDICE E – *script de backup*

```
#!/bin/bash
# =====
# objetivo: backup dos arquivos de configuração
# autor: Dorival Junior
# versão: 1.0
# =====
DATA=$( /bin/date )
/bin/cp /etc /root/backup_etc
/bin/tar -cjvf /root/backup_etc-$(DATA).tar.bz2 /etc
/usr/sbin/scp -p 62333 /root/backup_etc-$(DATA).tar.bz2
/djunior@10.0.0.2:backup_etc_firewall
/bin/rm -rf backup_etc-$(DATA).tar.bz2
```

APENDICE F – *script para sincronização com servidor NTP*

```
#!/bin/bash
# =====
# objetivo: sincronização com servidor NTP publico
# autor: Dorival Junior
# versao: 1.0
# =====

NTPserver="ntp.cais.rnp.br"

# sincronizando com servidor NTP publico
/usr/sbin/ntpdate $NTPserver

# sincronizando o relógio do sistema para o hardware
/sbin/hwclock -w
```

ANEXOS

ANEXO A – autorização da empresa Contabilidade Dorival Machado e Filhos para a publicação dos resultados e procedimentos realizados

Contabilidade Dorival Machado e Filhos

Organização e Assessoria Contábil-Jurídica de Empresas em Geral - Uma Família a Seu Serviço
☎(35)3531-1919 / 4911 – www.dorival.com.br

AUTORIZAÇÃO

DORIVAL MOREIRA MACHADO, advogado, contador, titular da empresa CONTABILIDADE DORIVAL MACHADO E FILHOS, com sede na rua Geraldo Marcolini, 559, vila Santa Maria, nesta cidade de São Sebastião do Paraíso-MG, CEP 37950-000, autorizo a publicação dos resultados obtidos referente à monografia “**Proposta de Hardening em Conformidade com a ISO 27001 para um Firewall em Linux com Balanceamento de carga**” de autoria de **DORIVAL MOREIRA MACHADO JUNIOR**, implementada nesta empresa.

Autorizo ainda a publicação dos procedimentos de *hardening* realizados, regras de balanceamento e *firewall*, com exceção de algumas regras específicas e portas de serviços utilizados na instituição.

São Sebastião do Paraíso-MG, 26 de agosto de 2008


DORIVAL MOREIRA MACHADO

ANEXO B – autorização da instituição LIBERTAS – Faculdades Integradas para a publicação dos resultados e procedimentos realizados



AUTORIZAÇÃO

Professora Mestra Bernadeth Resende Torres, Diretora Pedagógica da Libertas – Faculdades Integradas, mantida pela **FUNDAÇÃO EDUCACIONAL COMUNITÁRIA DE SÃO SEBASTIÃO DO PARAÍSO**, com sede na Av. Wenceslau Brás, 1018, bairro Lagoinha, na cidade de São Sebastião do Paraíso-MG, CEP 37950-000, juntamente com o Chefe do Departamento de Tecnologia da Informação Davidson Scarano, autorizam a publicação dos resultados obtidos referente à monografia “**Proposta de Hardening em Conformidade com a ISO 27001 para um Firewall em Linux com Balanceamento de Carga**” de autoria de **DORIVAL MOREIRA MACHADO JUNIOR**, implementada nesta instituição.

Autoriza ainda a publicação dos procedimentos de *hardening* realizados, regras de balanceamento e firewall, com exceção de algumas regras específicas e portas de serviços utilizados na instituição.

São Sebastião do Paraíso-MG, 19 de agosto de 2008

Davidson Scarano
Departamento de TI

Bernadeth Resende Torres
Diretora Pedagógica

Mantenedora:

Fundação Educacional Comunitária
de São Sebastião do Paraíso

0800 283 2400 - www.fecom.edu.br

CNPJ: 24.903.999/0001-47

Av. Wenceslau Braz, 1.018 / 1.038 - CEP 37950-000 - São Sebastião do Paraíso/MG