Instruções para o suporte aos Produtos e Serviços que o Interlegis disponibiliza

http://colab.interlegis.gov.br/wiki/SustentacaoProdutosInterlegis

Equipe Interlegis
28 de outubro de 2008

Sobre este Manual

Este manual tem como objetivo servir de referência para os usuários de infra-estrutura, para realização de manutenção e instalação dos produtos Interlegis. Estes usuários podem ser tanto funcionários do Legislativo, como qualquer cidadão que tenha interesse nos sistemas que o Interlegis disponibiliza.

Foi construído, utilizando o Termo de Referência 128247 pelo consultor Halison do Nascimento Casimiro, que utilizou como referência as revisões feitas por:

- SSTIN/SPDT
  - Jean Ferri
- GITEC
  - Comunidade
  - Ângelo Marcondes de Oliveira Neto
- Colaboradores dos manuais do
  - SAAP
  - SAPL
  - Portal Modelo

Além de informações geradas a partir da interação dos membros da comunidade de Tecnologia do Interlegis (GITEC), disponibilizadas em http://listas.interlegis.gov.br/pipermail/gitec/, e de informações coletadas junto à equipe técnica do Interlegis, responsável pela gestão dos produtos.

Sumário

Capítulo 1 - Introdução

O objetivo dessas instruções é dar subsídio ao administrador da infra-estrutura, para realizar manutenção e instalação dos produtos: o Portal Modelo, o Sistema de Apoio ao Processo Legislativo (SAPL) e o Sistema de Apoio à Atividade Parlamentar (SAAP), deixando-os em bom funcionamento e otimizando as suas funcionalidades.

As funcionalidades e procedimentos para a instalação dos produtos e otimização, serão descritas e exemplificadas neste documento também por meio de diagramas e ilustrações.

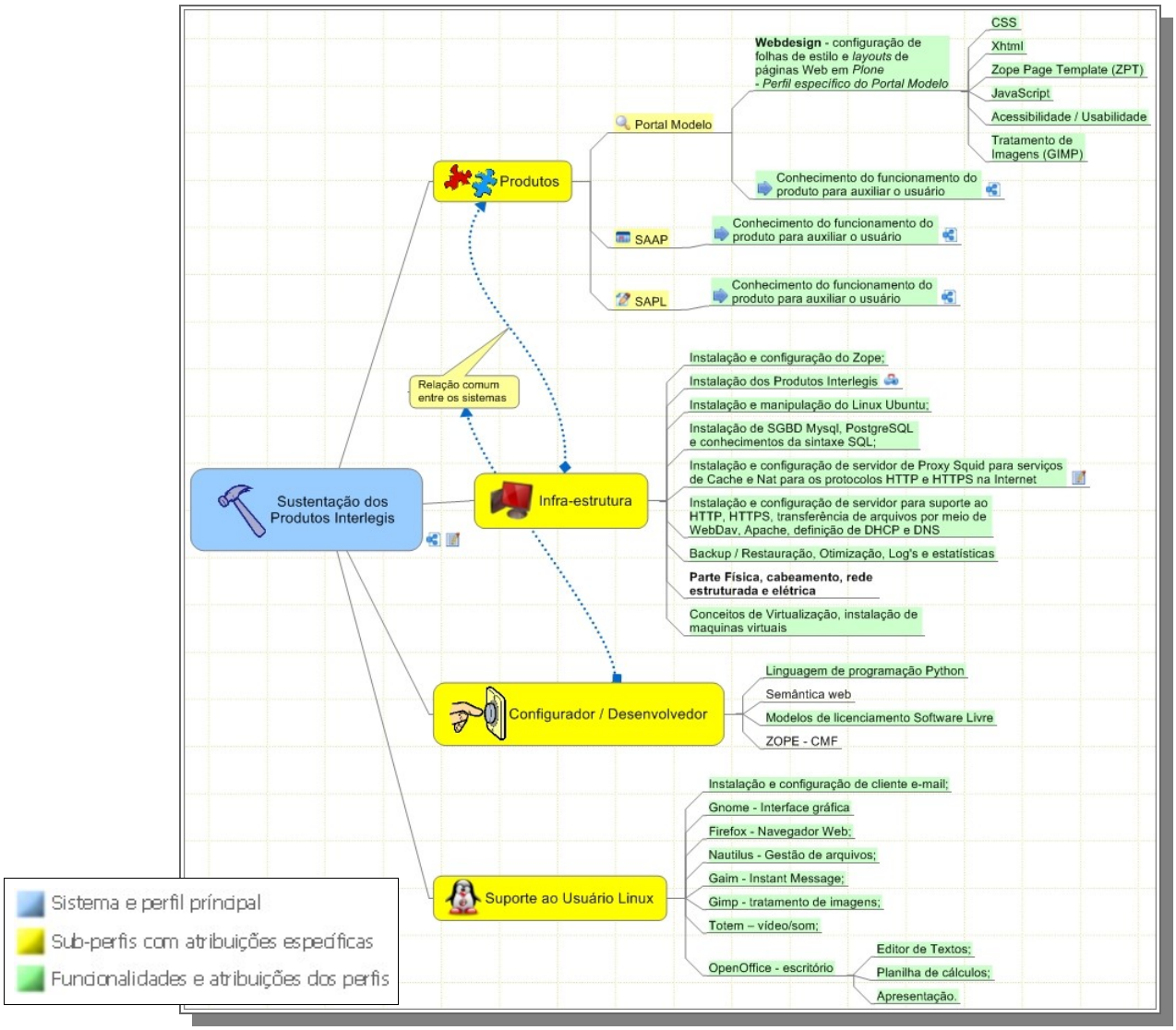
```
Este guia deve ser usado como orientação junto com os produtos a serem
prestadas as devidas instruções.

É destinado ao usuário que irá configurar, instalar, prestar manutenção nos
produtos. Para à administração de conteúdo e gestão dos sistemas, deve-se
utilizar os respectivos manuais dos sistemas.
```

Capítulo 2 - Perfil que proverá a sustentação dos produtos do Interlegis.

Objetivo: dar sustentação aos processos, procedimentos e funcionalidades específicas de cada sistema do Interlegis.

Atribuições: execução de toda requisição da infra-estrutura, relacionada a: instalação, atualização, manutenção, e qualquer atividade ligada ao funcionamento dos produtos Interlegis, é executada por este perfil. Para classificar as atividades deste perfil, o mesmo foi sub-dividido em 4 (quatro) sub-perfis, como mostra a ilustração abaixo:



Capítulo 3 - Apresentação

1) Sobre o Interlegis

O Programa Interlegis, desenvolvido pelo Senado Federal em parceria com o Banco Interamericano de Desenvolvimento (BID), desde 1997, tem o objetivo de modernizar e integrar o Poder Legislativo brasileiro. Em 2005 o Programa foi promovido a Secretaria Especial no Senado Federal.

O Interlegis foi criado como agente facilitador do processo de integração e modernização do poder legislativo brasileiro, em suas instâncias federal, estadual e municipal, com o objetivo de melhorar a comunicação e o fluxo de informações entre os legisladores, aumentar a eficiência e competência das casas legislativas e promover a participação cidadã nos processos legislativos. Conta com a seguinte infra-estrutura, produtos e serviços:

- ✓ A **Rede Nacional *Interlegis* (RNI)** integrando os estados por videoconferência, telefonia e dados e os municípios pela Internet, formando uma comunidade virtual (Comunidade *Interlegis*) e dotando o Poder Legislativo do País da infra-estrutura tecnológica adequada para o suporte ao Programa.

- ✓ A rede de **videoconferências** do Interlegis: serviço de transmissão de áudio e vídeo (*vídeo streaming*) via internet. Instrumento de comunicação com as Assembléias Legislativas e têm atendido não só ao Poder Legislativo, mas também ao Executivo, Judiciário e a organismos internacionais, como o Banco Mundial.

- ✓ Criada uma vigorosa **comunidade** formada por servidores das Casas Legislativas, chamada *GITEC – Grupo Interlegis de Tecnologia*, que desde 2004 dá sustentação aos principais produtos desenvolvidos. Atualmente, com a efetiva participação do *GITEC*, que é fortemente focado em Tecnologia, já estão criadas e em funcionamento outras Comunidades de Prática especializadas por áreas de interesse. O *GIAL – Grupo Interlegis de Assessoria Legislativa* e *o GICOM – Grupo Interlegis de Comunicação*. A Comunidade *GICAP – Grupo Interlegis de Capacitação* está em processo de criação.

- ✓ Desenvolvidos um conjunto de produtos, desenhados especialmente para o Legislativo, com a participação efetiva de servidores do legislativo de todos os recantos do País. Os produtos desta parceria são muitos, e de valor inestimável. Em primeiro lugar, através do processo de trabalho colaborativo em rede, através das Comunidades de Prática; servidores de todo o País, se relacionam, trocam experiências e aprendem. Este relacionamento garante o crescimento profissional de todos e é uma alavanca poderosa para a Modernização das Casas Legislativas. Além disso, os Sistemas de Informação desenvolvidos estão em constante e franca evolução através do seu uso por essa Comunidade, que o validam, sugerem melhorias e até desenvolvem novas funcionalidades. Atualmente, estão disponíveis os seguintes produtos:

- SAPL – **Sistema de Apoio ao Processo Legislativo**, para apoiar e normatizar as ações desenvolvidas no âmbito do Processo Legislativo.

- Portal Modelo – É o Ponto de presença da Casa Legislativa na Internet. Este produto é um importante veículo de comunicação, e, é por meio dele, que a Casa Legislativa disponibiliza ao cidadão, toda a sua produção legislativa, bem como a de seus parlamentares.

- SAAP – Sistema de Apoio à Atividade Parlamentar. Disponibiliza um conjunto de

procedimentos integrados para apoio às tarefas relativas à atividade parlamentar.

Para acompanhar o que está sendo discutido nas casas legislativas basta acessar o Portal Interlegis: www.interlegis.gov.br. A página é atualizada diariamente com notícias variadas de interesse dos estados e municípios brasileiros.

2) Como Participar da Comunidade Interlegis

O Interlegis fornece um canal de participação para a Comunidade Legislativa no desenvolvimento e na utilização dos seus produtos.

O COLAB é o portal colaborativo para a gerência dos projetos de software do Interlegis. Seu objetivo é apresentar num único local todo o processo do desenvolvimento dos softwares e a sua documentação, acrescendo atualizações, novas funcionalidades, boas práticas, dicas e experiências das Casas Legislativas. Enfim, dando uma visão geral dos produtos e de todo o ambiente técnico disponível para a Comunidade do Legislativo. Visite o endereço: http://colab.interlegis.gov.br.

O principal veículo de comunicação da Comunidade são **as listas de discussão**. Uma lista de discussão é um serviço no qual os usuários interessados cadastram o seu endereço de e-mail, e passam a receber mensagens sobre o assunto daquela lista. Cada mensagem enviada por um usuário da lista é distribuída, pelo servidor de listas, para todos os usuários participantes da lista.

Atualmente estão disponíveis para a Comunidade Interlegis três listas de discussão. São elas:

A lista de discussão **GITEC** – Grupo Interlegis de Tecnologia é o canal oficial de suporte ao uso, de solução de problemas e de sugestão de melhorias aos produtos de software desenvolvidos pelo Interlegis. É também um canal para a comunicação e a troca de experiências entre os seus membros com relação à informatização de Casas Legislativas: em janeiro de 2008 já são mais de 250 associados, de todas as regiões do Brasil. Para ver mais detalhes sobre o **GITEC** acesse http://www.interlegis.gov.br/comunidade/comunidade-gitec.

A lista de discussão **GIAL** – Grupo Interlegis de Assessoria Legislativa é composta por membros da Comunidade Legislativa interessados na discussão sobre o Processo Legislativo e suas várias formas de utilização, seguindo as regras estabelecidas nas Constituições Federal, Estadual e Municipal e no Regimento Interno das Casas Legislativas. Para ver mais detalhes sobre o **GIAL** acesse http://www.interlegis.gov.br/comunidade/comunidade-gial.

A lista de discussão **GICOM** – Grupo Interlegis de Comunicação é composta por membros da Comunidade Legislativa ligados às questões que envolvem os processos de comunicação das casas legislativas, tais como assessoria de imprensa, jornalismo, relações públicas, publicidade, consultoria de comunicação e imagem, rádio e televisão. Para ver mais detalhes sobre o **GICOM** acesse http://www.interlegis.gov.br/comunidade/comunidade-gicom.

Além das Listas de Discussão, outra importante ferramenta, o **MENSAGEIRO**, é utilizada para comunicação individualizada entre dois membros da Comunidade. Esta ferramenta possibilita a troca de mensagens instantâneas, facilitando a comunicação entre os membros da comunidade GITEC. Para informações sobre que cliente utilizar, acesse o endereço: http://colab.interlegis.gov.br/wiki/FAQ

a) Melhores práticas no uso de listas de discussões

Uma lista de discussão deve ser utilizada com responsabilidade. Por isto foram listadas algumas dicas para seu uso:

- ✓ Envie mensagens **pessoais** direto para o (a) destinatário (a);
- ✓ Escreva mensagens detalhadas, porém objetivas sobre seu problema;
- ✓ Evite o envio de anexos nas mensagens;
- ✓ Use formatação texto puro, não HTML, para compor suas mensagens;
- ✓ Escreva normalmente com letras maiúsculas e minúsculas. NÃO GRITE!
- ✓ Não repasse correntes, spams e similares para a lista;
- ✓ Sempre preencha o assunto (subject) na mensagem, coerente com o seu propósito;
- ✓ Tenha cuidado com a linguagem que você utiliza. Palavras de baixo calão e ofensas são condenadas pelos moderadores;
- ✓ Se você estiver com alguma dúvida, tente antes buscar a solução no histórico da lista: http://genesis.interlegis.gov.br/tecnologia/lista
- ✓ Se não encontrar a solução, envie seu questionamento para os endereços gitec@listas.interlegis.gov.br, ou gial@listas.interlegis.gov.br ou gicom@interlegis.gov.br.

Capítulo 4 - Conceitos dos produtos

1) Base de conhecimento sobre os produtos

SAPL – **Sistema de Apoio ao Processo Legislativo**, para apoiar e normatizar as ações desenvolvidas no âmbito do Processo Legislativo, sendo um agente efetivo de modernização, de melhoria da qualidade das Leis produzidas, e integração tanto com o Executivo como com a população, que pode acompanhar a tramitação das Matérias de seu interesse, bem como a produção legislativa da Casa e dos Parlamentares.

Portal Modelo – É o Ponto de presença da Casa Legislativa na Internet. Este produto é um importante veículo de comunicação, e, é por meio dele, que a Casa Legislativa disponibiliza ao cidadão, toda a sua produção legislativa, bem como a de seus parlamentares. Além disso, estabelece um canal direto com o cidadão através do mecanismo de Ouvidoria, de modo a permitir a ele – cidadão – solicitar e propor ações aos seus representantes. Tecnicamente falando, é um sistema para publicação de diversos tipos de conteúdo (documentos, imagens, links[1], notícias, eventos, etc.) na Internet. Todas as informações da Casa Legislativa são elaboradas e publicadas, aumentando a transparência de suas atividades e a interação com a sociedade através de meios de busca aos documentos publicados no portal, criação de chats[2], fóruns, pesquisas de opinião e etc.

SAAP – Sistema de Apoio à Atividade Parlamentar. Disponibiliza um conjunto de procedimentos integrados para apoio às tarefas relativas à atividade parlamentar. Isso envolve principalmente os instrumentos de gerência das interações de parlamentares com pessoas, grupos e organizações de interesse. Tais instrumentos são: serviços de mala-direta; calendário; marcação de eventos; agendamento de reuniões; gestão de pleitos contemplando o recebimento da solicitação, o acompanhamento das ações relacionadas e o retorno ao solicitante do resultado final obtido e etc.

a) Quais serviços cada um oferece.

SAPL

Possui sua estrutura modular, podendo-se atribuir atividades para recursos diferentes. Os módulos são os seguintes:

- Módulo de Atualização da Mesa-Diretora
- Módulo de Atualização de Comissão
- Módulo de Atualização de Ordem-Dia
- Módulo de Manutenção de Parlamentares
- Módulo de Recebimento de Proposição
- Modulo de Matérias Legislativas
- Modulo de Normas Jurídicas
- Modulo de Relatórios
- Módulo de Tabelas Auxiliares

1 Link: é um texto que pode nos levar a textos, imagens e outros

2 Chat: que em português significa "conversação" ou "bate-papo"

- Elaboração e composição de proposição;

Portal Modelo

O Portal Modelo utiliza uma ferramenta[3] que possibilita a uma equipe com várias pessoas, com funções diferentes, em ambientes (computadores) diferentes, incluir, excluir, alterar e publicar conteúdos como:

- Elaboração e composição de matéria;
- Ferramenta de revisão de conteúdo;
- Notícias;
- Destaques;
- Eventos;
- Enquetes;
- Sistema de Ouvidoria
- Sistema de Boletim Eletrônico;
- Chats, Fóruns e Enquete.

SAAP

O sistema proporciona módulos para gestão de contatos, que auxilia nos cadastros de: *Pessoas Físicas, Pessoas Jurídicas, Formas de Tratamento, Profissões, Grupos, Tipos de Endereço, Tipos de Telefone, Tipos de Dependente.*

Também permite realizar buscas simples e avançadas, podendo incluir documentos, tópicos, e tipos de documentos. **Gerencia mala Direta**, Fontes de Dados e Modelos de conteúdo. Possui também a função no sistema que gerencia os **compromissos de Visitas**, Agendar Visita, Visualizar Visitas por Período, Tipos de Divulgação e Situações de Compromisso. **Agenda:** Gere tarefas e compromissos de agenda. Possui funcionalidades de: **Compromissos e Tarefas**, Tipos de Divulgação, Tipos de Compromisso, Situação de Compromisso, Situações de Tarefa e Tipos de Participação.

2) Dimensionamento de computadores para o funcionamento dos produtos

A especificação das máquinas é determinada pela configuração mínima, especificada abaixo para cada modelo de utilização do equipamento:

a) Servidores de Rede

Processador	Processador com arquitetura x86; Performance de Clock mínima de **1 GHz**;
Memória	Memória RAM do tipo DDR SDRAM DIMM com capacidade instalada de no mínimo **512 MB**.
Placa Principal	Mínimo de 2 (duas) portas USB versão 2.0. Uma interface Controladora de disco rígido integrada, padrão ATA ou SATA, Ultra DMA 100, ou superior, com suporte a no mínimo 04 periféricos, inclusive CD-ROM; Permitir o recurso de "wake-up on LAN" e "wake up on modem"; No mínimo 2 slots PCI 32 bits, versão 2.2. Um slot AGP 4x/8x ou um slot PCI Express.

3 **CMS** (Gestor de Conteúdo Web) por exemplo: o Plone.

Interface de vídeo	Interface de vídeo On-Board[4], com memória compartilhada de no mínimo 8MB. Poderá ser fornecida interface Off-Board[5] utilizando-se o barramento AGP ou PCI Express com placa de vídeo de no mínimo 8MB. Em qualquer dos casos deverão possuir drives específicos para Sistema Operacional Linux, distribuição UBUNTU LTS
Unidades de armazenamento	Uma unidade de disco rígido padrão ATA ou SATA; Capacidade mínima de armazenamento de no mínimo **10 GB**;
Monitor de Vídeo	Monitor de vídeo padrão SVGA policromático. Fonte de alimentação automática para 110 e 220 VAC.
Interface de Rede	Interface de rede padrão Gigabit ETHERNET com suporte a controle de fluxo Full Duplex (IEEE 802.3x), compatível com protocolos IEEE 802.3u e 803.3ab, suporte a priorização de tráfego (IEEE 802.1P) e suporte a VLAN (IEEE 802.1Q), saída 10BaseT/100BaseTX/1000BaseTX (RJ45), auto-sense.
Mouse Scroll	Mouse com resolução por hardware de no mínimo 400 dpi;
Teclado	Destacável do gabinete com teclas para movimentação do cursor e teclado numérico destacados, atendendo aos padrões das normas ABNT-2. Conector compatível com a placa principal, sem utilização de adaptador;
Gabinete padrão ATX	Fonte de alimentação com seleção de tensão bi-volt (110/220 V), automática ou manual; Com potência suficiente para suportar a máxima configuração do equipamento, mínimo 500w; Dotada de ventilação forçada; Cabo de força compatível com o estabilizador; A posição da fonte no gabinete não poderá cobrir, no todo ou parcialmente, o processador e seu respectivo ventilador. Ser do tipo torre ou *desktop;*
Unidade Leitor de DVD ou CD	Capacidade de Leitura de 16X CAV para DVD, 52X CAV para CD-ROM; Interface[6] padrão ATA ou superior; Interna ao gabinete; Acompanhar software de instalação para sistema operacional Linux.
Sistema Operacional	O sistema operacional dos equipamentos deste item será o Linux Ubuntu 5.10 ou, preferencialmente, a versão Ubuntu LTS;

b) Estações de Trabalho

Para a estação de trabalho, o equipamento mínimo é qualquer hardware que **suporte um navegador de Internet**.

Exemplo: Um computador com memória superior a 64mb, processador com freqüência mínima de 500mhz e espaço em disco rígido de 5gb. Com Sistema Operacional que Suporte Navegador de Internet, por exemplo o Firefox 1.0.

4 On-board vem diretamente conectado aos circuitos da placa mãe

5 Off-board não vem diretamente conectado aos circuitos da placa mãe, e sim em uma placa externa

6 Interface: é a fronteira que define a forma de comunicação entre duas entidades.

Capítulo 5 - Conceitos e pré-requisitos para a sustentação dos produtos

1) Sistema operacional Linux

É um software que permite a utilização da máquina por outros programas, ativando e gerenciando a memória, dispositivos de entrada e saída. Também conhecido É um conjunto de programas (rotinas) executado pelo processador que estabelece uma interface de contato do usuário com o computador e do computador com o usuário.

O sistema operacional utilizado como base para instalação dos produtos é o Ubuntu Linux; o **Ubuntu Linux** é um sistema operacional Linux gratuito, disponível com suporte técnico gratuito ou pago. E porque a utilização deste sistema operacional? Pois ele possui compromissos de **que o Ubuntu será sempre gratuito**. Não haverá pagamentos extra para versões melhoradas e que o software estará disponível para todos nos mesmos termos. **Uma nova versão a cada 6 meses**. Cada versão será suportada com atualizações de segurança e correção de erros por pelo menos 18 meses. O Ubuntu está totalmente empenhado com os **princípios do software livre** e encoraja as pessoas a usá-lo, melhorá-lo e passá-lo a outras pessoas.

A versão atual do Ubuntu é a 8.04, versão de Longo Tempo de Suporte (LTS) tem três anos de suporte para *desktops*, e cinco anos para servidores.

Utilizaremos como base na instalação dos servidores o Ubuntu *Server* LTS. O Ubuntu S*erver* LTS é uma versão do Ubuntu destinada a servidores, sem ambiente gráfico pré-instalado.

```
O Ubuntu Server é recomendado para usuários com alguns conhecimentos de
Linux e seus comandos de terminal.
```

2) Protocolos

É um conjunto de regras que especifica formatos, sincronismos e tratamento de possíveis erros na transmissão de dados entre computadores. Iremos ver neste capítulo os protocolos relacionados a instalação e manutenção dos servidores web.

3) TCP/IP

Os **protocolos TCP/IP** são um conjunto de protocolos de comunicação entre computadores em rede. Seu nome vem dos dois protocolos mais importantes do conjunto: o TCP (Transmission Control Protocol - Protocolo de Controle de Transmissão) e o IP (Internet Protocol - Protocolo de Interconexão). O conjunto de protocolos pode ser visto como **um modelo de camadas,** onde cada camada é responsável por um grupo de tarefas, fornecendo um conjunto de serviços bem definidos para o protocolo da camada superior. As camadas mais altas estão logicamente mais perto do usuário (camada de aplicação), e lidam com dados mais abstratos, confiando em protocolos de camadas mais baixas para tarefas de menor nível de abstração. Resumidamente, o modelo é o que podemos chamar de uma *"solução prática para problemas de transmissão de dados"*.

a) Endereçamento

A configuração do protocolo TCP/IP consiste em diversos elementos, que podem ser editados

nos arquivos de configuração apropriados, ou optando-se por soluções como o servidor de DHCP (Protocolo de Configuração Dinâmica de *Hosts (endereços)*), que por sua vez pode ser configurado para **prover** as configurações TCP/IP necessárias **para cada cliente de rede** automaticamente.

Os elementos básicos de configuração do TCP/IP e seus objetivos são os seguintes:

- **Endereço IP** O Endereço de IP é uma *string*[7] de identificação única, expressa em quatro números decimais, que vão de zero (0) à duzentos e cinqüenta e cinco (255), separada por pontos, com cada um dos quatros números representado oito (8) bits do endereço, para um tamanho total de trinta e dois (32) bits para todo o endereço. Este formato é chamado de *notação decimal com pontos*.

- **Máscara de Rede** A Máscara de Subrede (ou simplesmente *netmask*) é uma máscara de bits[8] locais, ou alguns marcadores que separam porções de endereços IPs relacionados à uma rede de uma *subrede*. Por exemplo, na Classe C, a máscara padrão é 255.255.255.0, que mascara os primeiros três bytes[9] do endereço IP e permite somente o último byte do endereços disponível para a alocação e especificação de hosts[10] ou subredes.

- **Endereço de Rede** O Endereço de rede representa os bytes compreendidos na porção de rede referente a um IP. Por exemplo, o host 12.128.1.2 da rede de Classe A, pode usar 12.0.0.0 como o Endereço de Rede, que usa o doze (12) para representar o primeiro byte de um endereço IP, (a parte de rede) e zeros (0s) em todos os outros três bytes restantes para representar os valores para hosts em potencial. Redes de hosts usando endereços IPs comuns como os privados e não distribuídos, como 192.168.1.100 pode então usar um endereço de rede como 192.168.1.0, que especifica os três primeiros bytes para a Classe C de rede 192.168.1 e zero (0) para todos os outros possíveis hosts da rede.

- **Endereço de Transmissão** O Endereço de Transmissão é um endereço IP que possibilita dados de rede serem enviados simultaneamente para todos os hosts numa subrede, preferivelmente do que especificar um host particular da rede. O padrão genérico de endereço de transmissão para redes IP é 255.255.255.255, mas este endereço de transmissão não pode ser usado para enviar uma mensagem a cada host na Internet porque roteadores bloqueiam-no. Por exemplo, em um popular IP privado Classe C de rede, 192.168.1.0, o endereço de transmissão precisa ser configurado como 192.168.1.255. Transmissão de mensagens são tipicamente fruto de rede de protocolos tais como *Address Resolution Protocol (ARP)* e *Routing Information Protocol (RIP)*.

- **Gateway Address** Um Gateway Address é o endereço IP direto de uma rede particular, ou host em uma rede, podendo se estender. Se uma rede de host não define-se ao comunicar com outra rede de host, e aquele host não é localizado em uma mesma rede, então um *gateway* deve ser usado. Em muitos casos, o Gateway Address será de um roteador na mesma rede, que vai habilitar o tráfego de passagem em outras redes ou hosts, tais como Internet hosts. O valor definido a um Gateway Address deve ser correto, ou seu sistema não será capaz de alcançar nenhum host ligado na mesma rede.

7 String: Grupo de caracteres alfanumérica, qualquer combinação de letras, números e símbolos

8 Bit (simplificação para dígito binário, “BInary digiT” em inglês) é a menor unidade de medida de transmissão de dados

9 Byte: Conjunto de "bits" que representam um único caracter. Cada byte possui oito bit

10 Host é qualquer máquina ou computador conectado a uma rede

b) Endereço do Servidor de Nomes (DNS)

Endereços de servidores de nome representam o endereço IP do sistema de Serviço de Nomes de Domínio (Domain Name Service - DNS), que resolve nomes de hosts de rede para endereços IP. Há três níveis de endereços de servidor de nomes, que podem ser especificados em ordem de precedência: O servidor de nomes *Primário*, o servidor de nomes *Secundário* e o servidor de nomes *Terciário*. Para que seu sistema possa resolver nome de hosts da rede para seus endereços IP correspondentes, você deve especificar um endereço de servidor de nomes válido o qual você esteja autorizado a utilizar na configuração de TCP/IP do seu sistema. Em muitos casos esses endereços podem e devem ser fornecidos pelo seu provedor de serviços de rede, mas há muitos servidores de nomes gratuitos e acessíveis publicamente, como os servidores Level 3 (Verizon) com endereços de IP de 4.2.2.1 a 4.2.2.6.

4) Máscara de rede

A máscara de rede especifica a gama de IPs — domínio de colisão — que pode ser abrangida por um determinado endereço, e é especialmente necessária no processo de encaminhamento (*roteamento*). Ainda, com simples cálculos, pode-se gerir eficientemente o espaço de endereçamento disponível.

A notação formal de uma máscara de rede é o formato típico de um endereço IP e, aplicada com uma operação AND *(onde uma idéia tem de ser verdadeira (igual a 1) em ambas as situações (conjuntos) para que o resultado seja verdadeiro)* sobre um endereço IP, devolve a rede a que este pertence. Por exemplo,

```
  192.168. 20.5     =      11000000.10101000.00010100.00000101
& 255.255.255.0     =      11111111.11111111.11111111.00000000
---------------            ----------------------------------
  192.168. 20.0     =      11000000.10101000.00010100.00000000
```

Ou seja, o IP 192.168.20.5 pertence, aparentemente, à rede 192.168.20.0. Para simplificar a representação, convencionou-se que a máscara de rede poderia acompanhar o IP especificando o número de bits '1' contíguos, separada por uma barra '/'. Por exemplo, a rede anterior podia ser representada como 192.168.20.0/24.

O espaço de endereçamento também é ditado pela máscara de rede, e é equivalente à negação dos seus bits a '0', exceptuando o primeiro e último endereço (endereços de rede e *broadcast*[11], respectivamente). Por exemplo, uma máscara de 255.255.255.192 irá disponibilizar 62 endereços.

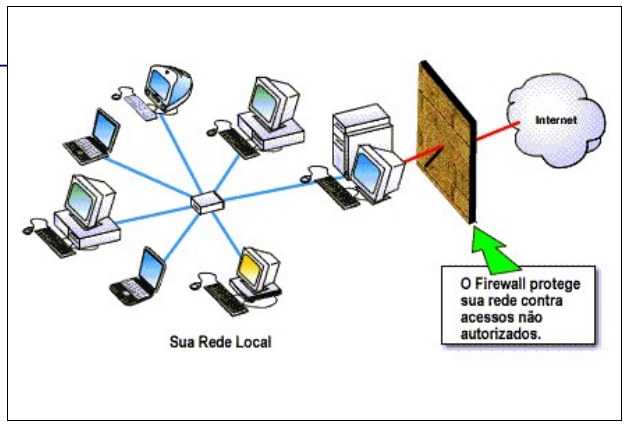
5) Domain Name Service (DNS)

O Serviço de Nomes de Domínio (DNS) é um serviço de Internet que liga endereços IP e nomes de domínio totalmente qualificados (FQDN) uns aos outros. Computadores que rodam DNS são chamados de *servidores de nomes*. O Ubuntu possui o **BIND** (Berkley Internet Naming Daemon), o programa mais comumente usado para manter um servidor de nomes em GNU/Linux.

11 Broadcast: Uma transmissão enviada a mais de um receptor

6) FIREWALL

Firewall é o nome dado a todo o esforço, elemento, dispositivo de uma rede de computadores que tem por objetivo **aplicar uma política de segurança** a um determinado ponto de controle da rede. Sua função consiste em regular o tráfego de dados entre redes distintas e impedir a transmissão e/ou recepção de acessos nocivos ou não autorizados de uma rede para outra. Este conceito inclui os equipamentos de filtros de pacotes e de *proxy* de aplicações, comumente associados a redes TCP/IP.



Os primeiros sistemas *firewall* nasceram exclusivamente para suportar segurança no conjunto de protocolos TCP/IP (*ver história*).

O termo inglês *firewall* faz alusão comparativa da função que este desempenha para evitar o alastramento de acessos nocivos dentro de uma rede de computadores à uma parede corta-fogo (*firewall*), que evita o alastramento de incêndios pelos cômodos de uma edificação[1].

Existe na forma de *software* e *hardware*, ou na combinação de ambos (neste caso, normalmente é chamado de "appliance"). A complexidade de instalação depende do tamanho da rede, da política de segurança, da quantidade de regras que autorizam o fluxo de entrada e saída de informações e do grau de segurança desejado.

a) Tipos de esforços para controle de segurança

Os sistemas *firewall* podem ser classificados da seguinte forma:

Filtros de Pacotes

Estes sistemas analisam individualmente os pacotes à medida em que estes são transmitidos, verificando as informações das camada de enlace (camada 2 do modelo ISO/OSI) e de rede (camada 3 do modelo ISO/OSI).

As regras podem ser formadas indicando os endereços de rede (de origem e/ou destino) e as portas TCP/IP envolvidas na conexão. A principal desvantagem desse tipo de tecnologia para a segurança reside na falta de controle de estado do pacote, o que permite que agentes maliciosos possam produzir pacotes simulados (com endereço IP falsificado, técnica conhecida como IP Spoofing), fora de contexto ou ainda para serem injetados em uma sessão válida. Esta tecnologia foi amplamente utilizada nos equipamentos de 1ª Geração (incluindo roteadores), não realizando nenhum tipo de decodificação do protocolo ou análise na camada de aplicação.

Proxy Firewall ou *Gateways* de Aplicação

Os conceitos de *gateways*[12] de aplicação (*application-level gateways*) e "bastion hosts" foram introduzidos por Marcus Ranum em 1995. Trabalhando como uma espécie de eclusa, o *firewall*

12 Gateway: Computador ou material dedicado que serve para interligar duas ou mais redes

de *proxy*[13] trabalha recebendo o fluxo de conexão, tratando as requisições como se fossem uma aplicação e originando um novo pedido sob a responsabilidade do mesmo *firewall* (*non-transparent proxy*) para o servidor de destino. A resposta para o pedido é recebida pelo *firewall* e analisada antes de ser entregue para o solicitante original.

Os *gateways* de aplicações conectam as redes corporativas à Internet através de estações seguras (chamadas de *bastion hosts*) rodando aplicativos especializados para tratar e filtrar os dados (os *proxy firewalls*). Estes *gateways*, ao receberem as requisições de acesso dos usuários e realizarem uma segunda conexão externa para receber estes dados, acabam por esconder a identidade dos usuários nestas requisições externas, oferecendo uma proteção adicional contra a ação dos *crackers*[14].

Desvantagens

- Para cada novo serviço que aparece na Internet, o fabricante deve desenvolver o seu correspondente agente de *Proxy*. Isto pode demorar meses, tornando o cliente vulnerável enquanto o fabricante não liberta o agente específico. A instalação, manutenção e atualização dos agentes do *Proxy* requerem serviços especializados e podem ser bastante complexos e caros;
- Os *proxies* introduzem perda de desempenho na rede, já que as mensagens devem ser processadas pelo agente do *Proxy*. Por exemplo, o serviço FTP[15] manda um pedido ao agente do *Proxy* para FTP, que por sua vez interpreta a solicitação e fala com o servidor FTP externo para completar o pedido;
- A tecnologia atual permite que o custo de implementação seja bastante reduzido ao utilizar CPUs de alto desempenho e baixo custo, bem como sistemas operacionais abertos (Linux), porém, exige-se manutenção específica para assegurar que seja mantido nível de segurança adequado (ex.: aplicação de correções e configuração adequada dos servidores).

Firewall de Aplicação

Com a explosão do comércio eletrônico, percebeu-se que mesmo a última tecnologia em filtragem de pacotes para TCP/IP poderia não ser tão efetiva quanto se esperava. Os ataques passaram a se concentrar nas características (e vulnerabilidades) específicas de cada aplicação. Foi desenvolvido um novo método que pudesse analisar as particularidades de cada protocolo e tomadas de decisões que pudessem evitar ataques maliciosos contra uma rede.

Se comparado com o modelo tradicional de *Firewall* -- orientado a redes de dados, o *Firewall* de Aplicação é frequentemente instalado junto à plataforma da aplicação, atuando como uma espécie de procurador para o acesso ao servidor (Proxy).

Alguns projetos de código-aberto, como por exemplo o ModSecurity[2] para servidores Apache, têm por objetivo facilitar a disseminação do conceito para as aplicações Web.

Vantagens

- Pode suprir a deficiência dos modelos tradicionais e mapear todas as transações específicas que acontecem na camada da aplicação Web proprietária;
- Por ser um terminador do tráfego SSL, pode avaliar hipertextos criptografadas (HTTPS)

13 Proxy: Servidor que atua como intermediário entre um cliente e outro servido

14 Cracker é o termo usado para designar quem pratica a quebra (ou cracking) de um sistema de segurança, de forma ilegal ou sem ética

15 File Transfer Protocol (FTP) significa protocolo de transferência de arquivos pela Internet

que originalmente passariam despercebidos ou não analisados por *firewalls* tradicionais de rede;

Desvantagens

- Pelo fato de embutir uma grande capacidade de avaliação técnica dos métodos disponibilizados por uma aplicação (Web), este tipo de *firewall* exige um grande poder computacional -- geralmente traduzido para um grande custo de investimento;
- Ao interceptar aplicações Web e suas interações com o cliente (o navegador de Web), pode acabar por provocar alguma incompatibilidade no padrão de transações (fato que exigirá, sem sombra de dúvidas, um profundo trabalho de avaliação por parte dos implementadores);
- Alguns especialistas ou engenheiros de tecnologia refutam o *firewall* de aplicação baseando-se nas seguintes argumentações:
    - A tecnologia introduz mais um ponto de falha sem adicionar significativos avanços na tecnologia de proteção;
    - O *firewall* e o IDS/IPS já seriam suficientes para cobrir grande parte dos riscos associados a aplicação Web;
    - A tecnologia ainda precisa amadurecer o suficiente para ser considerada um componente indispensável de uma arquitetura de segurança.

Certamente esses argumentos serão bastante discutidos ao longo dos próximos anos como um imperativo para determinar a existência desta tecnologia no futuro.

Mascaramento de IP

O propósito da Máscara de IP é permitir máquinas com IP privado, endereço não-roteável em sua rede para acessar a Internet por meio da máquina "mascarada". O tráfico destinado de sua rede privada para a Internet deve ser manipulado para obter respostas da máquina que fez a petição, como em uma rota invertida. Para fazer isto, o *kernel*[16] deve modificar o endereço IP da *fonte* de cada pacote e retornar respostas a ele, antes que o endereço privado IP faça o pedido de resposta, que é impossível através da Internet. O Linux usa *Connection Tracking* (conntrack) para acompanhar que conexões pertence a que máquinas e desviar cada pacote de retorno correspondente. O tráfico originado em sua rede privada é assim "mascarado" como tendo originado de seu gateway Ubuntu.

b) Boas práticas

Ferramentas

Há muitas ferramentas disponíveis para ajudá-lo a construir um firewall completo sem conhecimento íntimo da ferramenta iptables. Para os que preferem GUI (interfaces gráficas), sugere-se o **Firestarter** é bem popular e de fácil utilização, e o **fwbuilder**, uma aplicação poderosa com visual familiar para administradores que usam ferramentas comerciais de firewall, como o Checkpoint FireWall-1. Se você preferir uma ferramenta em linha de comando para configurar arquivos em "texto puro", o **Shorewall** é uma solução poderosa que o ajudará em configurações avançadas de firewall em sua rede. Se sua rede for relativamente simples ou você não possuir uma rede o **ipkungfu** deve proporcionar-lhe um firewall útil com configuração inicial zero, e o permitirá facilmente armar um firewall mais avançado editando arquivos de configuração simples e bem documentados. Outra ferramenta interessante é o

16 Kernel: Camada que contém os comandos de um sistema operacional ou de uma rede

fireflier, que é orientado para *desktop*. É composto de um servidor (fireflier-server) e sua escolha de clientes GUI (GTK ou QT).

Exemplos

Fazendo o IP forward

para estabelecermos o IP *forward*[17] entre duas redes, bastará:

- inserir um micro com duas placas de rede entre as duas redes, configurando cada placa de acordo com cada rede;
- definir, em cada máquina, de cada rede, quem é o seu gateway;
- Para definir o gateway em cada cliente devemos editar o arquivo /etc/network/interfaces e inserir, no final da configuração da placa de rede a linha:

```
gateway ip_do_gateway
```

Exemplo:

```
auto eth0
iface eth0 inet static
      address 10.0.0.1
      netmask 255.0.0.0
      network 10.0.0.0
      broadcast 10.255.255.255
      gateway 10.0.0.10
```

- Em seguida, reiniciar a rede:

```
# /etc/int.d/networking restart
```

O Mascaramento de IP

Pode ser realizado com uma única regra no *iptables*, que pode diferir levemente baseado em sua configuração de rede:

```
sudo iptables -t nat -A POSTROUTING -s 192.168.0.0/16 -o ppp0 -j MASQUERADE
```

O comando acima supõe que seu endereço privado está no intervalo 192.168.0.0/16 e sua interface de Internet, ou dispositivo, é ppp0. A sintaxe é errada como se segue:

- -t nat -- a regra é para ir na tabela nat
- -A POSTROUTING -- a regra é para ser adicionada (-A) à corrente POSTROUTING
- -s 192.168.0.0/16 -- a regra é aplicada a trafego originando do endereço especificado
- -o ppp0 -- a regra é aplicada a trafego agendado para ser roteado pelo dispositivo de rede especificado
- -j MASQUERADE -- trafego combinando com esta regra "pulará" (-j) para o alvo MASQUERADE para ser manipulado como descrito acima

Cada série na tabela de filtro (a tabela padrão, onde a maioria ou todos os processos e filtragem de pacotes ocorre) tem uma *diretriz* padrão para ACEITAR, mas se você estiver criando um

17 Forward: encaminhar

firewall adicional para o dispositivo de gateway, você terá que definir políticas de DESCARTE ou REJEIÇÃO, em que caso seu tráfico "mascarado" necessitará de permissão pra ENVIAR para a série de regras de trabalho acima:

```
sudo iptables -A FORWARD -s 192.168.0.0/16 -o ppp0 -j ACCEPT
sudo iptables -A FORWARD -d 192.168.0.0/16 -m state --state
ESTABLISHED,RELATED -i ppp0 -j ACCEPT
```

Os comandos acima permitem todas conexões de sua rede local à Internet e todo trânsito relacionado a essas conexões retornar à máquina que os iniciou.

Logs

O registro (log) das ações do firewall é essencial para reconhecer ataques, investigar e reparar erros em suas regras do firewall e notar atividades inesperadas na rede. Você deve incluir regras de registro em seu firewall para que registros sejam gerado, aliás, e regras de registro devem vir antes de qualquer regra aplicável (uma regra com um alvo que decida o destino do pacote, tal como ACEPT, DISCARD ou REJECT). Por exemplo:

```
sudo iptables -A INPUT -m state --state NEW -p tcp --dport 80 -j LOG --log-
prefix "NEW_HTTP_CONN: "
```

As requisições pela porta 80 para a máquina local, então, geraria um registro *dmesg* parecido com este:

```
[4304885.870000]            NEW_HTTP_CONN:            IN=lo            OUT=
MAC=00:00:00:00:00:00:00:00:00:00:00:00:08:00  SRC=127.0.0.1  DST=127.0.0.1
LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=58288 DF PROTO=TCP SPT=53981 DPT=80
WINDOW=32767 RES=0x00 SYN URGP=0
```

O registro acima é publicado em `/var/log/messages`, `/var/log/syslog`, e `/var/log/kern.log`. Estes procedimentos podem ser alterado modificando o `/etc/syslog.conf` ou instalando e configurando o **ulogd** e, assim, usar o ULOG como alvo ao invés do LOG (registro). O daemon **ulogd** é um servidor userspace que observa o sistema para registrar instruções específicas do kernel para firewalls e registrar qualquer arquivo que você queira, igual aos bancos de dados **PostgreSQL** e **MySQL**. O registro das ações do firewall pode ser simplificada usando uma ferramenta para análise de registros, como o **fwanalog**, **fwlogwatch**, ou **lire**.

c) Política de Segurança

Ao fazer um estudo em políticas de segurança utilizadas em algumas instituições, foi identificado a utilização de organismos que regulamentam essas políticas. Com base nessas políticas, são propostas orientações de boas práticas:

O que temos que preservar?

A informação; ela é um Bem que, como todo Bem importante do negócio tem valor para a instituição e conseqüentemente necessita ser devidamente protegida.

Aonde está a informação?

Escritas ou impressas em papel; eletronicamente armazenadas; transmitidas por meios eletrônicos; mostradas em vídeos corporativos e faladas em conversas.

Como fazer a segurança?

Fazer a segurança dessas Informações é um processo de gerenciamento, não um processo tecnológico. Iremos fazer esse gerenciamento mantendo eficazes a **integridade** da informação a **disponibilidade** dela e em alguns casos a **confidencialidade** da informação.

Veja os conceitos de cada diretriz:

Integridade: Proteger a exatidão da informação e dos métodos de processos.

Disponibilidade: Assegurar que usuários autorizados tenham acesso a informações e recursos associados quando requeridos.

Confidencialidade: Assegurar que a informação é acessível somente àqueles autorizados a ter acesso. **Em algumas instituições (alguns setores públicos) essa diretriz não é tão importante** pois não faz parte de sua concepção.

Como preservar as diretrizes

Usando de premissas e **recomendações** básicas de segurança como:

Educação sobre segurança: Se o usuário conhece os problemas ele irá se afastar deles ou pelo menos teme-los. Segundo Kevin Mitnick (http://pt.wikipedia.org/wiki/Kevin_Mitnick|) "*A falha de segurança é na maior parte das vezes relacionado ao material humano. Os próprios funcionários, voluntária ou involuntariamente são o elo fraco na segurança de uma rede!!!*". Nada melhor que a educação para solucionar esses problemas.

Sobre deveres e direitos: Se o usuário tiver conhecimentos de quais são os seus deveres como servidor público ele em tese procurará cumpri-los, deixar os direitos sempre disponíveis e nunca omiti-los. No ato da contratação, fazer o funcionário ler e entender uma declaração de confidencialidade, se for o caso, das informações da instituição, da integridade, isso inclui o uso indevido do patrimônio físico e lógico, incluindo o uso da rede de dados para satisfação pessoal.

Motivação: Motivar o servidor (funcionário) a utilizar o seu tempo de navegação com boas práticas, onde ele possa ganhar uma melhor performance, ter uma melhora no nível de satisfação dos seus clientes e melhorar o seu currículo.

Regras: Se existirem regras sobre o que pode, o que não pode e o que as vezes pode ser trafegado na rede, simplesmente algum problemas podem ser resolvidos. O acesso a Internet também possui regras; Limitar acesso a sites não relacionados ao trabalho, recomenda-se o bloqueio das portas de download de músicas, sites de relacionamento, pornográficos e afins, downloads[18] em geral não relacionados ao trabalho.

Base sólida: Se sua base de trabalho é sólida você estará menos propenso a problemas na rede, ou seja, seu Sistema Operacional tem que ser seguro, as ferramentas de trabalho que norteiam todos os processos tem que seguir linhas de segurança. Manter sempre os produtos

18 Download (significa descarregar, em português), é a transferência de dados de um computador remoto para um computador local

computacionais atualizados para evitar falhas de segurança. Recomenda-se utilização de **software livre** em todos os seguimentos.

Integridade: Baseia-se em fazer controles e oferecer recomendações de segurança como:

- Controles físicos: são barreiras que limitam o contato ou acesso direto a informação ou a infra-estrutura (que garante a existência da informação) que a suporta. Existem mecanismos de segurança que apóiam os controles físicos: Portas / trancas / paredes / blindagem / guardas / etc ..

- Controles lógicos: são barreiras que impedem ou limitam o acesso a informação, que está em ambiente controlado, geralmente eletrônico, e que, de outro modo, ficaria exposta a alteração não autorizada por elemento mal intencionado.

Existem mecanismos de segurança que apóiam os controles lógicos:

- *Mecanismos de criptografia*[19]. Permitem a transformação reversível da informação de forma a torná-la ininteligível a terceiros. Utiliza-se para tal, algoritmos determinados e uma chave secreta para, a partir de um conjunto de dados não criptografados, produzir uma seqüência de dados criptografados. A operação inversa é a decifração.
- *Assinatura digital*. Um conjunto de dados criptografados, associados a um documento do qual sua função é garantir a integridade do documento associado, **mas não a sua confidencialidade.**
- *Mecanismos de garantia da integridade da informação*. Usando funções de "*Hashing*[20]" ou de checagem, consistindo na adição.
- *Mecanismos de controle de acesso*. Palavras-chave, sistemas biométricos, firewalls, cartões inteligentes.
- *Mecanismos de certificação*. Atesta a validade de um documento.
- *Integridade*. Medida em que um serviço/informação é genuíno, isto é, está protegido contra a **personificação** por intrusos.
- *Honeypot*: É o nome dado a um software, cuja função é detectar ou de impedir a ação de um cracker, de um spammer[21], ou de qualquer **agente externo** estranho ao sistema, enganando-o, fazendo-o pensar que esteja de fato explorando uma vulnerabilidade daquele sistema.

Existe hoje em dia um elevado número de ferramentas e sistemas que pretendem fornecer segurança. Alguns exemplos são os detectores de intrusões, os anti-vírus, firewalls, firewalls locais, filtros anti-spam, fuzzers[22], analisadores de código, etc.

Lembre-se, desde que essas recomendações não "**engessem**" o trabalho ou retardem o bom funcionamento dos processos, elas devem ser seguidas como forma de manter a Integridade, disponibilidade e confidencialidade.

19 Criptografia: transformação reversível da informação de forma a torná-la ininteligível a terceiros

20 **Hashing** - É uma forma de se implementar e intuitiva de se organizar grandes quantidades de dados. Permite armazenar e encontrar rapidamente dados por chave.

21 Spam, abreviação em inglês de "spiced ham" (presunto condimentado), é uma mensagem eletrônica não-solicitada enviada em massa

22 Fuzzers: injetores, as vezes de codigos.

Capítulo 6 - Instalação do servidor

1) Instalar Ubuntu Server LTS

Passo inicial é o download do cd http://old-releases.ubuntu.com/releases/; a versão do Ubuntu 5.10 é a recomendada para os servidores dos produtos Interlegis.

Grave o arquivo .iso em um CD-ROM utilizando um software gravador de CD. Caso tenha dificuldade conheça o processo mais detalhadamente; acesse http://wiki.ubuntu-br.org/ComoGravarImagemIso.

Após realizar o download e gravar a imagem em um CD, configure seu computador para *bootar*[23] pelo CD (normalmente é o padrão). Um requisito importante desta tutorial é que você deve estar conectado na Internet.

O instalador do Ubuntu é de fácil entendimento e utilização, mas caso tenha dificuldades para conhecer o processo mais detalhadamente acesse http://wiki.ubuntu-br.org/GuiaIntrodutorio/LinuxIniciando/ExperimenteLinux.

Insira seu CD de instalação no seu drive de CD-ROM e reinicie seu computador. O sistema de instalação é inicializado imediatamente ao ser feito *boot* pelo CD-ROM. Uma vez inicializado, sua primeira tela aparecerá.

Neste momento, leia o texto na tela. Você pode querer ler a tela de ajuda fornecida pelo sistema de instalação. Para fazer isto, pressione F1.

Para executar uma instalação padrão de servidor, selecione “Instalar no disco rígido” e pressione **Enter**. O processo de instalação será inicializado. Simplesmente siga as instruções apresentadas na tela, e seu sistema Ubuntu será instalado

Alternativamente, para instalar um servidor LAMP (Linux, Apache, MySQL, PHP/Perl/Python), selecione “Instalar um Servidor LAMP ”, e siga as instruções.

Vídeos na Internet podem auxiliar neste processo:

http://video.google.com/videosearch?q=particionar+hd&emb=0#emb=0&q=instala%C3%A7%C3%A3o%20do%20ubuntu

a) Recomendação para particionamento

Uma partição é uma divisão de um disco rígido, o sistema operacional Linux precisa de 2(duas) partições, uma para armazenamento de arquivos do sistema operacional e dos arquivos (musica, documentos, imagens e etc) do usuário, e outra para otimização do sistema. Uma é chamada EXT2, que é um sistema de arquivo com segurança e otimizado; a outra e o SWAP, que é um arquivo de troca. É um arquivo, criado no disco rígido, usado pelo sistema operacional para simular memória RAM, sempre que a memória física se esgotar.

SWAP

Simplesmente a SWAP não precisa ter o dobro do tamanho da memória RAM, isso não é uma

23 Boot é o termo em inglês para o processo de iniciação do computador

lei;

1. O tamanho da SWAP variará de acordo com as seguintes variáveis
    1. Quantidade de RAM disponível;
    2. Quantidade de disco rígido disponível;
    3. Consumo de memória pelas aplicações utilizadas na Estação ou Servidor.

Concluindo, a SWAP deverá ser atribuída de acordo com o perfil do usuário e de seu computador. Uma dica fica para os usuários com sistemas que necessitam de uma grande quantidade de recurso, que sempre mantenham uma boa quantidade de SWAP, afinal de contas os sistemas tem múltiplas áreas de trabalho, que dá pra abrir um monte de aplicações.

Acessar arquivos de outro Sistema Operacional

Para tal, pode-se utilizar o "Ext2 IFS For Windows", que nada mais é que um IFS (Instalable File System) para Windows NT4.0/2000/XP/2003/Vista com acesso completo aos volumes Ext2 permitindo leitura e gravação dos arquivos. Sabendo que o Ext3 possui a mesma estrutura do Ext2 com o recurso adicional de journaling (que faz o computador recuperar mais facilmente se for desligado sem que se desmonte corretamente os volumes) então ele serve para os dois tipos de sistemas de arquivos.

Vamos ao que interessa, entre no site [http://www.fs-driver.org/] e baixe a última versão na aba Download. Durante a instalação (que pode ser observada no site pela aba Screenshots[24]) as seguintes questões precisarão ser respondidas:

1. "Enable the read-only option?" - Habilite caso queira montar os volumes apenas em modo de leitura evitando que o Windows (ou o usuário) faça qualquer alteração no sistema de arquivos do Linux.

2. "Enable UTF-8 encoding?" - A maioria das distribuições Linux usa o padrão UTF-8 para acentuação, se você não marcar ele vai usar o padrão do Windows, que normalmente é ISO-8859-1.

3. "Enable large file feature?" - Normalmente habilitado permite a gravação de arquivos maiores que 2Gb, em discos com kernel até a versão 2.2 (ainda bem que a maioria das versões atuais usam o kernel 2.6) esse suporte não existia, se for o seu caso desmarque a opção, a criação de um arquivo com mais de 2Gb faz com que o Linux não consiga montar o volume novamente.

4. Por último você pode fazer a associação das suas partições Ext2/Ext3 com as letras de drives do Windows, exite nesta tela (que pode ser acessada posteriormente pelo painel de controle) uma opção para vincular automaticamente novos volumes Ext2/Ext3 às unidades do Windows, isso é útil para quem usar pendrives ou HD's externos via USB com sistemas de arquivos Linux.

2) Configurar rede

A maior parte da configuração de rede está centralizada em um único arquivo, `/etc/network/interfaces`. Se você não possui dispositivos de rede, somente a interface loopback[25] aparecerá neste arquivo, e será parecido com isto:

24 Screenshots: imagem mostrada no monitor gravada em um arquivo ou num arquivo.

25 Loopback é um canal de comunicação com apenas um ponto final. Qualquer mensagem transmitida por meio de tal

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback
address 127.0.0.1
netmask 255.0.0.0
```

Se você tiver apenas um dispositivo de rede, eth0, e este estiver obtendo a configuração via servidor DHCP, ele pode ser carregado automaticamente durante o *boot*, para isso, bastam apenas duas linhas adicionais:

```
auto eth0
iface eth0 inet dhcp
```

A primeira linha específica que o dispositivo *eth0* deve ser habilitado automaticamente durante o *boot*. A segunda linha diz que a interface ("*iface*") eth0 deve ter um espaço *IPv4* (substitua "*inet*" por "*inet6*" para dispositivos *IPv6*) e isto deverá obter automaticamente a configuração via DHCP. Assumindo que sua rede e servido DHCP já esteja devidamente configurado, esta máquina não precisará de nenhuma configuração adicional para funcionar corretamente. O servidor DHCP irá prover o gateway padrão (implementado através do comando **route**), os endereços de IP (implementados com o comando **ifconfig**), e os servidores DNS usados na rede (implementados no arquivo `/etc/resolv.conf`.).

Para configurar sua interface de rede *ethernet*[26] com um IP estático e uma configuração personalizada, será necessário algumas informações. Suponhamos que você queira definir o IP 192.168.0.2 para a interface eth1, com a máscara de rede típica 255.255.255.0. Seu gateway (rota de saída) padrão é 192.168.0.1. Você deverá inserir algo como isto no arquivo `/etc/network/interfaces`:

```
iface eth1 inet static
        address 192.168.0.2
        netmask 255.255.255.0
        gateway 192.168.0.1
```

Neste caso, você precisará especificar o endereço dos servidores de DNS manualmente no arquivo `/etc/resolv.conf`, que deverá parecer com algo do tipo:

```
search mydomain.com
nameserver 192.168.0.1
nameserver 4.2.2.2
```

A diretiva *search* vai anexar *mydomain.com* para a procura de *hostnames*, tentando resolver nomes para sua rede. Por exemplo, se o domínio de sua rede é *meudominio.com* e você tentar fazer um ping[27] no host "*meucomputador*", a procura pelo DNS será modificada para "*meucomputador.meudominio.com*". A diretiva *nameserver* especifica os servidores DNS a serem usados para resolver os *hostnames* para o IP. Se você usa um *nameserver* (servidor DNS)

canal é imediatamente recebida

26 Ethernet é uma tecnologia de interconexão para redes locai

27 Ping é um comando usado pelo protocolo ICMP para testar a conectividade entre equipamentos

próprio, insira-o aqui. Senão, pergunte ao seu provedor de internet os servidores DNS primário e secundário, e depois insira-os em `/etc/resolv.conf`, como mostrado abaixo.

Diversas outras configurações são possíveis, incluindo interfaces PPP, rede em IPv6, interfaces VPN, entre outras. Execute o comando **man 5 interfaces** para mais informações e para as opções suportadas. Lembre-se que `/etc/network/interfaces` é utilizado pelos *scripts* **ifup**/**ifdown** como um esquema de configuração de mais alto nível, que pode ser utilizado por outras distribuições, e que os utilitários de baixo nível, como **ifconfig**, **route** e **dhclient** continuam disponíveis para configurações *ad hoc*.[28]

3) Manter Atualizado (Gerenciador de Pacotes)

Uma característica do Ubuntu é um sistema que facilita o gerenciamento de pacotes, sua instalação, atualização, configuração e remoção de software. Além de fornecer acesso a uma base organizada de mais de 17.000 pacotes de software para seu computador Ubuntu, o Gerenciador de Pacotes também inclui a capacidade de resolução de dependência e procura por atualizações de software.

O comando **apt-get** é uma poderosa ferramenta de trabalho presente no Ubuntu. *Advanced Packaging Tool* (APT) ou Avançada Ferramenta de Pacotes, possui funcionalidades tais como instalação de novos pacotes de software, atualização de pacotes existentes, atualização da lista de pacotes e atualização do sistema Ubuntu como um todo.

- **Atualizando a Lista de Pacotes**: A lista de pacotes do APT é essencialmente um bando de dados com os pacotes disponíveis em repositórios definidos no arquivo `/etc/apt/sources.list`.

```
Para instalar ou atualizar os sistemas que a Interlegis disponibiliza, atualize o sources.list
Para instalá-los, vá no interpretador de comando do linux 1º substitua o arquivo /etc/apt/sources.list (faça o dowload neste link: http://colab.interlegis.gov.br/wiki/SourcesList) utilizando um editor de textos VI ou gedit.
```

- Após atualizar a lista de repositório, para atualizar a lista local de pacotes com as últimas alterações feitas no(s) repositório(s), digite:

```
sudo apt-get update
```

- **Atualizando Todos os Pacotes do Sistema**: Com o tempo, versões atualizadas de pacotes atualmente instalado em seu computador podem tornar-se disponíveis nos repositórios de pacotes (atualizações de segurança, por exemplo). Para atualizar seu sistema, primeiro atualize a base de dados de pacotes e então digite:

```
sudo apt-get upgrade
```

Se um pacote necessitar, na atualização, que seja instalada ou removida uma nova dependência, ele não será atualizado pelo comando *upgrade*. Para tal use:

```
sudo apt-get dist-upgrade.
```

28 Ad hoc: Significa literalmente: para isto, para este fim específico.

4) Registros (log)

Alguns produtos do Interlegis, utilizam o servidor ZOPE[29] **(Plone[30])**, este não possuir um produto específico para intelegibilidade de auditoria de conteúdo, porém, é possível auditar o conteúdo que é manipulado nestas instancias através do arquivo **Z2.log**. Este é um arquivo de log[31] , que contém as ocorrências de autenticação, inclusão e alteração de conteúdo, registrando informações de usuário, endereçamento IP e data/horário.

Existem os seguintes comando para manipular esses arquivos:

Caso queira listar todo o conteúdo do arquivo Z2.log

```
$cat /var/log/zope2.8/portalcasas/Z2.log
```

Caso queira listar as dez ultimas linha do arquivo Z2.log

```
$tail /var/log/zope2.8/portalcasas/Z2.log
```

Caso precise monitorar o log em tempo de execução, como um trace ou um "Debug" on-line, inclua a opção "-f"

```
$tail -f /var/log/zope2.8/portalcasas/Z2.log
```

Caso queira listar somente as linhas que contenham o termo 192.168.0.1

```
$cat /var/log/zope2.8/portalcasas/Z2.log | grep 192.168.0.1
```

Obs: Aprenda mais sobre comando linux em [http://www.vidalinux.com.br/archives/24]

Caso possua Apache ou Squid na frente do Portal Modelo (PM), precisará utilizar os logs desses servidores para auditoria, pois no PM, será logado apenas o endereço IP do *front-end*[32].

Outro recurso bastante útil nesse sentido, é o *portlet* "alterações recentes" que mostra o que, quando e por quem foi inserido ou alterado os conteúdos mais novos.

Sistemas

Um bom sistema para análise estatística e gráfica do Portal Modelo e outros sistemas do Interlegis é o AWStats, que pode analisar o *log* do *Zope*, do *Apache* e até do *Squid*.

5) Configurar NTP (horário)

O NTP (Protocolo de tempo mundial) é um protocolo usado para sincronismo de relógio com servidores, computadores e roteadores na Internet.

29 Zope é um servidor de aplicações web Open Source escrito na linguagem Python

30 Plone é um Sistema de Gerenciamento de Conteúdo (CMS, de Content Management System) escrito na linguagem Python

31 Log de dados, registro de eventos em um sistema de computadores

32 Front-end é a parte do sistema de software que interage diretamente com o usuário

Para manter o horário sempre atualizado eu use o seguinte comando:

```
$ sudo apt-get install ntp-server
```

No arquivo /etc/ntp.conf acrescentar:

```
server ntp.cais.rnp.br
```

Quem não quiser instalar o *ntp-server* pode fazer apenas:

```
$ sudo apt-get install ntpdate
$ sudo ntpdate ntp.cais.rnp.br
```

Ou acrescentar em /etc/default/ntpdate a linha:

```
NTPSERVERS="ntp.cais.rnp.br"
```

E para atualizar o fuso para o horário de verão instale o pacote

```
sudo apt-get install tz-brasil
```

Quando reiniciar a estação o horário estará atualizado.

Capítulo 7 - Instalação do produto

Neste item serão exploradas todas as formas de instalação dos Produtos Interlegis, para atender as diferentes necessidades. São elas:

- Instalação em uma máquina servidora
- Instalação em uma estação de trabalho
- Instalação para uso em sala de aula

1) Instalar produto (Portal, SAPL ou SAAP) em uma maquina servidora

a) Para produção (Publicação)

A instalação dos Produtos sobre o sistema operacional Ubuntu, pode ser realizada de várias maneiras, dentre estas temos:

- Apt-get (repositório)
- Subversion
- CD-ROM.

Neste tutorial, faremos à instalação dos Produtos, utilizando o *apt-get*, que é maneira, mais fácil, prática e utilizada. Caso você não conheça o conceito de trabalho do *apt-get*, consulte o Capítulo: Manter Atualizado (Gerenciador de Pacotes) ou este tutorial em http://www.guiadohardware.net/tutoriais/tutorial-completo-apt-get/, onde encontrará a definição bem como uma excelente explanação sobre o software e sua utilização.

Para realizarmos o processo de instalação, necessitaremos verificar alguns itens:

- Ter a senha de administrador;
- Estar conectado a Internet;
- Utilizar uma das versões de Ubuntu suportadas (5.04, 5.10, 6,10 e 7.04).

Estando com todos os itens OK, vamos partir para o processo de configuração:

```
Se já foi executado a atualização de repositório ignore este passo, execute
as orientações para instalação.
```

Inicialmente realizaremos uma cópia de segurança do arquivo "*sources.list*", que será modificado no próximo item, para isso vá até o terminal e digite:

```
$ sudo cp /etc/apt/sources.list /etc/apt/orig-sources.list
```

Com a cópia de segurança do *source.list* realizada, vamos a passo onde substituiremos o conteúdo do arquivo original pelo modificado com os repositórios dos produtos Interlegis adicionados, para isso vá ao terminal e digite:

```
sudo gedit /etc/apt/sources.list
```

Abra o *link*[33] correspondente na caixa abaixo, selecione todo o conteúdo e copie:

33 Link: é um texto que pode nos levar a textos, imagens e outros

- Versão 7.04 (feisty) em http://colab.interlegis.gov.br/attachment/wiki/HOWTO-InstalarSAPLUbuntu/sources.list.txt
- Versão 6.10 (edgy) em http://ftp.interlegis.gov.br/pub/interlegis/produtos/ubuntu/sources-list/6.10-edgy/sources.list
- Versão 5.10 (breezy) em http://ftp.interlegis.gov.br/pub/interlegis/produtos/ubuntu/sources-list/5.10-breezy/sources.list
- Versão 5.04 (hoary) em http://ftp.interlegis.gov.br/pub/interlegis/produtos/ubuntu/sources-list/5.04-hoary/sources.list

Retorne ao **gedit**, apague todo o conteúdo do arquivo e cole o **conteúdo** copiado.

Posteriormente salve as alterações e feche o aplicativo.

Tendo realizado as alterações em nosso *sources.list*, vamos atualizar a sua base de pacotes, para isso vá até o terminal e digite:

```
$ sudo apt-get update
```

Agora, vamos a instalação em si,

Para instalar o Sistema de Apoio ao Processo Legislativo (SAPL)

Para isso ainda no terminal digite:

```
$ sudo apt-get install sapl
```

Quando surgir a pergunta "*Instalar esses pacotes sem verificação?*", responda afirmativamente.

Durante o processo de instalação será solicitada a definição do *username* e da *senha* do usuário que ficará como administrador do *Zope*.

```
É muito importante guardar esta senha!
```

Para a instalação no Ubuntu 6.10 ou 5.10, será dada a opção de escolha da porta *tcp* a ser alocada para o SAPL. No Ubuntu 5.04, a porta adotada é a **8080**.

Apenas para o Ubuntu 6.10, após a escolha da porta, aparecerá uma pergunta similar a "*Deseja MANTER os dados de configuração do pacote quando for executado um PURGE?*". Responda NEGATIVAMENTE.

Apenas para o Ubuntu 5.10, após a escolha da porta, aparecerá uma pergunta similar a "*Deseja REMOVER os dados de configuração do pacote quando for executado um PURGE?*". Responda AFIRMATIVAMENTE.

O processo de instalação faz o download de um grande conjunto de pacotes (*Zope, MySQL,* etc...), dependendo do que já esteja instalado no sistema. Portanto, pode ser demorado. Aguarde até o aparecimento da mensagem "*Instalando sapl (2.1.0-1)..."*

Teste o funcionamento do sistema abrindo um navegador web e digitando, na barra de endereços: http://localhost:8080/sapl Este endereço para servidor, caso acesse outra maquina utilize http:<ip_do_servidor>:8080/sapl.

Para instalaro Portal Modelo das Casas Legislativas (PMCL)

Para isso ainda no terminal digite:

```
$ sudo apt-get install portal-modelo
```

Quando surgir a pergunta "*Instalar esses pacotes sem verificação?*", responda afirmativamente.

Durante o processo de instalação será solicitada a definição do *username* e da *senha* do usuário que ficará como administrador do Zope. É muito importante guardar esta senha!

Para a instalação no Ubuntu 6.10 ou 5.10, será dada a opção de escolha da porta tcp a ser alocada para o SAPL. No Ubuntu 5.04, a porta adotada é a 8180.

Apenas para o Ubuntu 6.10, após a escolha da porta, aparecerá uma pergunta similar a "*Deseja MANTER os dados de configuração do pacote quando for executado um PURGE?*". Responda NEGATIVAMENTE.

Apenas para o Ubuntu 5.10, após a escolha da porta, aparecerá uma pergunta similar a "*Deseja REMOVER os dados de configuração do pacote quando for executado um PURGE?*". Responda AFIRMATIVAMENTE.

O processo de instalação faz o download de um grande conjunto de pacotes (*Zope, MySQL,* etc...), dependendo do que já esteja instalado no sistema. Portanto, pode ser demorado. Aguarde até a finalização da instalação.

Teste o funcionamento do sistema abrindo um navegador web e digitando, na barra de endereços: http://localhost:8180/portal . Este endereço para servidor, caso acesse outra maquina utilize http:<ip_do_servidor>:8180/portal.

Para instalar o Sistema de Apoio a Atividade Parlamentar (SAAP)

Para isso ainda no terminal digite:

```
$ sudo apt-get install saap
```

Quando surgir a pergunta "*Instalar esses pacotes sem verificação?*", responda afirmativamente.

Durante o processo de instalação será solicitada a definição do *username*[34] e da *senha* do usuário que ficará como administrador do *Zope*. É muito importante guardar esta senha!

Para a instalação no Ubuntu 6.10 ou 5.10, será dada a opção de escolha da porta *tcp* a ser alocada para o SAPL. No Ubuntu 5.04, a porta adotada é a 8280.

Apenas para o Ubuntu 6.10, após a escolha da porta, aparecerá uma pergunta similar a "*Deseja MANTER os dados de configuração do pacote quando for executado um PURGE?"*. Responda NEGATIVAMENTE.

Apenas para o Ubuntu 5.10, após a escolha da porta, aparecerá uma pergunta similar a "*Deseja REMOVER os dados de configuração do pacote quando for executado um PURGE?"*. Responda AFIRMATIVAMENTE.

O processo de instalação faz o download de um grande conjunto de pacotes (*Zope, MySQL,* etc...), dependendo do que já esteja instalado no sistema. Portanto, pode ser demorado. Aguarde até a finalização da instalação.

Teste o funcionamento do sistema abrindo um navegador web e digitando, na barra de endereços: http://localhost:8280/saap . Este endereço para servidor, caso acesse outra maquina utilize http:<ip_do_servidor>:8280/saap.

34 Username: nome de usuário

2) Instalar produto a partir de uma maquina virtual

a) Para testes, estudo, experiências e etc.

O ideal para se trabalhar com os Produtos Interlegis é instalar a aplicação em um servidor e usa-la pela estação de trabalho como uma **aplicação web** (Cliente/Servidor, veja a definição em: http://pt.wikipedia.org/wiki/Aplicação_web), mas em alguns casos talvez seja necessário instalar os produtos na própria estação, como nos casos de:

- **Testes;**
- **Estudo;**
- **Salas de Aula**
- **Experimentação;**
- **Indisponibilidade de equipamento ou Sistema Operacional;**

Se este é o seu caso, poderemos realizar a instalação dos Produtos em sua estação de trabalho facilmente, mas para isso temos que preencher alguns requisitos:

- Saber qual é o sistema operacional utilizado;
- Possuir na estação 1 GB ou mais de memória RAM;
- Possuir 20GB livres no disco rígido;
- Possuir as seguintes informações sobre sua rede interna:
- Se os IPs são atribuídos automaticamente?
- Se negativo, qual é a faixa de IPs utilizada?

Instalação sobre Linux.

Caso a distribuição utilizada seja Ubuntu nas versões 5.04, 5.10, 6.10 e 7.04, basta seguir os procedimentos do item "*Instalação dos Produtos em uma máquina servidora*"

Caso a distribuição utilizada seja outra (*debian, madriva, redhat, slackware*, etc), ou poderemos instalar os Produtos facilmente utilizando uma **máquina virtual**[35] (veja a definição em: http://pt.wikipedia.org/wiki/Maquina_virtual).

Para isso, antes, é necessário o download e a instalação do software *Vmplayer* em sua estação de trabalho. Para baixar o *VMplayer* acesse o site do fabricante www.vmware.com.

Posteriormente a instalação do *VMplayer*, faça o download e a descompactação da máquina virtual com os produtos Interlegis para Linux disponíveis em: http://ftp.interlegis.gov.br/pub/interlegis/produtos/sistemas/SistemasInterlegis-vmware.tgz.

Para descompactar utilize o seguinte comando no terminal

```
$ tar -zxvf SistemasInterlegis-vmware.tgz
```

Posteriormente execute o *VMPlayer* e escolha o caminho onde está a máquina virtual que você

35 Maquina Virtual: Sistemas operacionais múltiplos sejam executados em um único computador ao mesmo tempo.

descompactou. Após a inicialização da máquina virtual, você poderá acessar os sistemas, mas antes precisará saber qual o endereço IP que o seu servidor DHCP deu à máquina virtual.

Para isso, faça *login* na máquina com os seguintes dados:

```
usuário: administrador
senha: interlegis
```

Então entre no terminal, na linha de comando digite o comando:

```
# ifconfig
```

Copie o endereço IP atribuído à interface eth0.

Caso sua rede não possua servidor DHCP, você poderá atribuir um IP fixo a máquina virtual, utilizando o comando:

"sudo ifconfig INTERFACE_DE_REDE(eth0) NUMERO_DO_IP(192.168.0.11) netmask MASCARA(255.255.255.0)". **Veja o exemplo:**

```
$ sudo ifconfig eth0 192.168.0.11 netmask 255.255.255.0
```

Para acessar os Produtos, vá até o navegador, digitando o endereço IP da máquina virtual em seu navegador. Algo como:

```
    * SAPL - http://ip_da_maquina_virtual:8080/sapl
    * Portal Modelo - http://ip_da_maquina_virtual:8180/portal
    * SAAP - http://ip_da_maquina_virtual:8280/saap
```

As informações para acessar os sistemas com o usuário administrador são:

```
SAPL
porta: 8080
usuário: admin
senha: interlegis

Portal Modelo
porta: 8180
usuário: admin
senha: interlegis

SAAP
porta: 8280
usuário: admin
senha: interlegis
```

Instalação sobre Windows.

Caso o sistema operacional utilizado seja *Windows*, poderemos instalar os Produtos facilmente utilizando uma **máquina virtual** (veja definição em: http://pt.wikipedia.org/wiki/Maquina_virtual).

Para isso antes se torna necessário o download e a instalação do software *VMplayer* em sua estação de trabalho. Para baixar o *VMplayer* acesse o site do fabricante www.vmware.com.

Posteriormente a instalação do *VMplayer*, faça o download e a descompactação da máquina virtual com os produtos Interlegis para Windows disponíveis em: http://ftp.interlegis.gov.br/pub/interlegis/produtos/sistemas/SistemasInterlegis-vmware.zip.

Para descompactar utilize um descompactador (*Winzip ou Izarc*)

Posteriormente execute o *VMPlayer* e escolha o caminho onde está a máquina virtual que você descompactou. Após a inicialização da máquina virtual, você poderá acessar os sistemas, mas antes precisará saber qual o endereço IP que o seu servidor DHCP deu à máquina virtual.

Para isso, faça login na máquina com os seguintes dados:

```
usuário: administrador
senha: interlegis
```

Então entre no terminal, na linha de comando digite o comando:

```
$ ifconfig
```

Copie o endereço IP atribuído à interface eth0.

Caso sua rede não possua servidor DHCP, você poderá atribuir um IP fixo a máquina virtual, utilizando o comando:

"sudo ifconfig INTERFACE_DE_REDE(eth0) NUMERO_DO_IP(192.168.0.11) netmask MASCARA(255.255.255.0)". **Veja o exemplo:**

```
$ sudo ifconfig eth0 192.168.0.11 netmask 255.255.255.0
```

Para acessar os Produtos, vá até o navegador, digitando o endereço IP da máquina virtual em seu navegador. Algo como:

```
    * SAPL - http://ip_da_maquina_virtual:8080/sapl
    * Portal Modelo - http://ip_da_maquina_virtual:8180/portal
    * SAAP - http://ip_da_maquina_virtual:8280/saap
```

As informações para acessar os sistemas com o usuário administrador são:

```
SAPL
porta: 8080
usuário: admin
senha: interlegis

Portal Modelo
porta: 8180
usuário: admin
senha: interlegis

SAAP
porta: 8280
usuário: admin
senha: interlegis
```

Observações:

A máquina virtual está configurada para consumir 256MB de memória e até 20GB de disco. Você pode alterar estes parâmetros para adequá-los ao seu hardware.

Se você pretende usar esta máquina virtual e os sistemas em produção, não esqueça de modificar as senhas.

3) Configuração do Zope

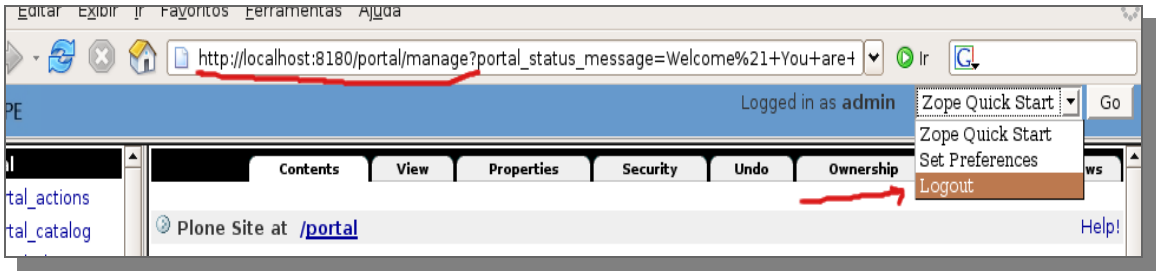
a) Acesso a interface de configuração

A Interface de configuração do *Zope* é chamada de ZMI (*Zope Management Interface*), Para acessa-la, digite a palavra manage no caminho do servidor:

```
http://<nome do servidor>:<porta>/<instância>/manage
http://localhost:8180/portal/manage
```

Sair da interface de configuração

Para sair da ZMI, no menu direito superior, clique na opção *Logout* como na figura acima.



b) Manutenção de senhas

Observações: Tais passos se referem ao *Zope* 2.8 que gerencia o SAPL 2.1, SAAP e o Portal Modelo

Criando um usuário temporário no *Zope*

1) Entre dentro da instância da qual quer criar a nova senha:

Exemplo:

```
$ cd /var/lib/zope2.8/instance/portalcasas #Portal Modelo
$ cd /var/lib/zope2.8/instance/sapl #SAPL
$ cd /opt/saap/zope #SAAP
```

2) Execute o seguinte comando:

Para o Portal Modelo e o SAPL:

```
$ sudo python /usr/lib/zope2.8/bin/zpasswd.py access
```

Para o SAAP:

```
$ sudo python zpasswd.py access
```

2.1)Crie o usuário

2.2)Defina a senha

3)Escolha o tipo de proteção da senha:

Selecione "SHA"

4)Vai aparecer uma questão sobre restrições do domínio *(Domain Restrictions):*

Só pressione ENTER, não precisa escrever nada.

5)Reinicie o Servidor Zope

Para o Portal Modelo e o SAPL:

```
$ sudo /etc/init.d/zope2.8 restart
```

Para o SAAP:

```
$ sudo /etc/init.d/saap restart
```

6)Acesse o ZMI com o usuário criando um novo usuário com "*papel*" de Administrador

7)Apague o arquivo *access* que foi criado dentro da instância (Passo 3)

c) Ligar, desligar e reinicializar o servidor.

Acesse a ZMI (*Item 1 deste capítulo)*

Para o Portal Modelo e o SAPL:

No console do sistema digite:

Para inicializar o servidor

```
$ sudo /etc/init.d/zope2.8 start
```

Reinicializar o servidor

```
$ sudo /etc/init.d/zope2.8 restart
```

Parar o servidor

```
$ sudo /etc/init.d/zope2.8 stop
```

Para o SAAP:

No console do sistema digite:

Para inicializar o servidor

```
$ sudo /etc/init.d/saap start
```

Reinicializar o servidor

```
$ sudo /etc/init.d/saap restart
```

Parar o servidor

```
$ sudo /etc/init.d/saap stop
```

Capítulo 8 - Configurações de otimização e performance

1) DNS (Bind)

Instalação

Em um terminal, digite o seguinte comando para instalar o **dns**:

```
sudo apt-get install bind
```

Configuração

Os arquivos de configuração do DNS são armazenados no diretório `/etc/bind`. O arquivo de configuração principal é o `/etc/bind/named.conf`. O conteúdo da configuração padrão está disposto abaixo:

```
// Este é o arquivo de configuração primária para o servidor de DNS BIND named.
//
// Por favor, leia /usr/share/doc/bind/README.Debian para informações sobre a
// estrutura dos arquivos de configuração do BIND no Debian para versão 8.2.1 do BIND
// ou superior, *ANTES* de você customizar este arquivo de configuração.
//

include "/etc/bind/named.conf.options";

// reduz a saída de log em erros fora do nosso controle
logging {
 category lame-servers { null; };
 category cname { null; };
};

// servidor primário, que conhece os servidores raiz
zone "." {
        type hint;
        file "/etc/bind/db.root";
};

// seja a autoridade para repasses locais, zonas reversas e para a
// zona de broadcast, como definido no RFC 1912

zone "localhost" {
        type master;
        file "/etc/bind/db.local";
};

zone "127.in-addr.arpa" {
        type master;
        file "/etc/bind/db.127";
};

zone "0.in-addr.arpa" {
        type master;
        file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
        type master;
        file "/etc/bind/db.255";
};

// adicione definições locais aqui
include "/etc/bind/named.conf.local";
```

A linha **include** especifica o nome do arquivo que contém as opções do DNS. A linha **directory** no arquivo de opções diz ao DNS onde procurar por arquivos. Todos os arquivos utilizados pelo BIND estão contidos nesse diretório.

O arquivo chamado `/etc/bind/db.root` descreve os servidores de nome raízes no mundo. Os servidores mudam com o tempo e precisam ser obtidos novamente e assim sempre.

A seção **zone** define um servidor mestre, e ela é armazenado em um arquivo mencionado através da tag file. Cada zona contém 3 registros de recursos (RRs): um RR SOA, um RR NS, e um RR PTR. SOA é a abreviatura para Start of Authority, ou seja, Início da Autoridade. A "@" é uma notação especial que denota a origem. NS é a RR para Servidor de Nomes. PTR é Ponteiro para Servidor de Nomes. Para iniciar o servidor DNS, rode o seguinte comando a partir do prompt de um terminal:

```
sudo /etc/init.d/bind start
```

2) Apache (**Virtual Host**)

Para deixar o Portal Modelo ou SAPL com a URL correta e bonita, algo como:

```
http://portalmodelo.interlegis.gov.br
```

Você precisa InstalarApache e configurar um VirtualHost.

Se a sua rede já sabe resolver o nome (URL) do Portal Modelo, SAPL, etc, ou seja, seu DNS já está configurado, você poderá criar um arquivo:

```
sudo vi /etc/apache2/sites-available/portalmodelo
```

E configurar o VirtualHost:

```
NameVirtualHost 10.10.10.10:80
<VirtualHost 10.10.10.10:80>
   ServerName portalmodelo.interlegis.gov.br
   ServerAlias portalmodelo
   ServerAdmin admin@portalmodelo.interlegis.gov.br
   CustomLog /var/log/apache2/access_portalmodelo.log combined
   ErrorLog /var/log/apache2/error_portalmodelo.log
   RewriteEngine On
   RewriteCond %{HTTP_HOST} ^([^:]+)(:|$)
          RewriteRule    ^(.*)$    http://localhost:8180/VirtualHostBase/http/
%1:80/portal/VirtualHostRoot$1 [P,L]
</VirtualHost>
```

Considerando que o Apache esteja no mesmo servidor que o Portal Modelo, esse *virtual host* passará todas as requisições que receber no domínio configurado para o Zope, com a URL[36] reescrita em conjunto com o *Virtual Host Monster* que deve estar habilitado na raiz do Zope.

Não esqueça de alterar todas as informações (IP, e-mail, nomes, portas, etc.) desse VirtualHost, adaptando-as para o seu caso.

Antes de habilitar o VirtualHost criado, você precisará habilitar os módulos *rewrite* e *proxy* do

36 URL: É o endereço de uma página na Web.

Apache, fazendo um link simbólico dos arquivos */etc/apache2/mods-available/rewrite.load* e */etc/apache2/mods-available/proxy.load* no seu respectivo diretório de módulos habilitados, o */etc/apache2/mods-enabled*. Para isso abra o terminal e digite:

```
$ cd /etc/apache2/mods-enabled
```

Para habilitar o módulo "proxy", digite no terminal:

```
$ sudo a2enmod proxy
```

Para habilitar o módulo "rewrite", digite no terminal:

```
$ sudo a2enmod rewrite
```

Considerando que você instalou o Apache 2, e esse VirtualHost foi criado no diretório */etc/apache/sites-available* basta habilitá-lo criando um link simbólico para o arquivo*/etc/apache/sites-avaliable/portalmodelo* no diretório */etc/apache/sites-enabled*. Para isso abra o terminal e digite:

```
$ cd /etc/apache2/sites-enabled
```

Para criar o link do "VirtualHost", digite o seguinte no terminal:

```
$ sudo ln -s /etc/apache2/sites-available/portalmodelo .
```

Apos feitas as configurações, reinicie o Apache e estará tudo funcionando. Para isso abra o terminal e digite:

```
$ sudo /etc/init.d/apache2 restart
```

Se sua rede não conhece o nome (URL) do SAPL você pode fazer de duas maneiras, através do arquivo */etc/hosts* ou através do DNS mesmo, que é o ideal.

3) Squid

a) O que é o Squid?

Squid é um **proxy-cache** de alta performance para clientes web, suportando protocolos FTP, gopher e HTTP[37].

O Squid mantém meta dados e especialmente objetos armazenados na RAM[38], cacheia buscas de DNS e implementa cache negativo de requests falhos.

Ele suporta SSL, listas de acesso complexas e *logging* completo. Por utilizar o *Internet Cache Protocol*, o Squid pode ser configurado para trabalhar de forma hierárquica ou mista para

37 HTTP (acrônimo para Hypertext Transfer Protocol, que significa Protocolo de Transferência de Hipertexto) é um protocolo de comunicação

38 RAM: A memória de acesso aleatório (Random Acess Memory) é a forma mais comum de memória de um computador

melhor aproveitamento da banda.

Podemos dizer que o Squid consiste em um programa principal - squid -,um sistema de busca e resolução de nomes - *dnsserver* - e alguns programas adicionais para reescrever *requests*[39], fazer autenticação e gerenciar ferramentas de clientes.

b) Instalar

Primeiro pegue o arquivo fonte do squid na página: [http://www.squid-cache.org/] Dê preferência as versões estáveis.

Depois descompacte o arquivo fonte:

```
tar -xzvf squid-versão.tar.gz
```

Pegue a patch para customizar o arquivo de **log** do squid em: [http://devel.squid-cache.org/old_projects.html#customlog]

Renomeie a pasta que foi descompactada para **squid**. Depois coloque a patch.

```
patch -p0 <customlog-2_5.patch
```

Entre na pasta do squid e configure a sua compilação.

```
cd  squid
./configure   --prefix=/usr/local/squid   --enable-gnuregex   --with-pthreads
--enable-storeio=ufs,aufs    --with-aufs-threads=10    --enable-useragent-log
--enable-referer-log   -enable-ssl   --enable-x-accelerator-vary   --with-dl
--enable-cache-digests
```

Veja que se for necessário outras configurações do squid elas poderão ser vistas utilizando o comando:

```
./cofigure --help
```

Depois que foi configurado entre como usuário **root**, pois o local que foi escolhido para instalar o squid só pode ser alterado pelo root e compile o *source*:

```
sudo su
make
```

Instale o squid

```
make install
```

Obs: Algumas vezes não será possível compilar o *source* por falta de algum pacote ou arquivo dos pacotes do debian, então veja qual o pacote ou arquivo que faltou e procure no site [http://debian.org], que lhe dirá qual o pacote que precisa ser instalado para poder compilar o *source*.

39 Request: Traduzindo para o português, significa **pedido,** ou seja são requisições de terceiros (cliente/servidor).

c) Configuração

Como comentado mais tarde, toda a estrutura do Squid é baseada em listas de acessos. Vamos entrar em detalhes mais para frente. Por hora vamos criar uma lista de acesso básica para nossos usuários.
Vamos supor que nossa rede interna seja 192.168.5.0/24. Crie a seguinte linha no squid.conf, na seção de ACLs (TAG: acl):

```
    acl rede_interna src 192.168.5.0/24
```

E a seguinte linha na seção de acesso (TAG: http_access)

```
    http_access allow rede_interna
```

O squid possibilita ser configurado como ferramentas de *firewall*, além de bloquear sites indesejados, para essas configurações acesse o link: http://www.linuxman.pro.br/node/1 para mais detalhes.

4) Cachefu

a) O que é

CacheFu é uma coleção de produtos que simplificam e agregar diferentes configurações de cache, acelerando Plone sites (Portal Modelo) usando uma combinação de memória, proxy e cache do navegador. CacheFu pode ser usado sozinho ou com o Squid, Varnish, e / ou Apache.

b) Instalar

Primeiramente abaixe o **CacheFu** com o subversion

```
svn co  http://svn.plone.org/svn/collective/CacheFu/trunk/CacheFu/ CacheFu
```

Depois pegue o modulo *memcached*

```
ftp://ftp.tummy.com/pub/python-memcached/
```

Descompacte-o e entre na pasta que foi criada

```
tar -xzvf python-memcached-1.2_tummy5.tar.gz
cd python-memcached-1.2_tummy5
```

Dentro da pasta, digite os seguintes comanda para que este modulo seja acrescentado no *python*[40] que sua instância zope utiliza:

```
../../pastadoseupython/bin/python setup build
../../pastadoseupython/bin/python setup install
```

40 Python é uma linguagem de programação de alto nível interpretada, interativa, orientada a objetos e de tipagem dinâmica e forte

c) Configuração

> Os procedimentos descritos abaixo pressupõem que os produtos tenha sido instalado em seu diretório padrão. Caso os produtos tenham sido instalados de forma diferente, ajuste os comandos adequadamente.

Depois de instalado o modulo, copie os produtos do **CacheFu** para dentro da pasta **Products** da sua instância zope. Feito isso, agora é só configurar o *squid:* Dentro da pasta *CacheFu* encontrará um pasta chamada **squid_direct**, nela encontrará os arquivos necessários para fazer o *squid* funcionar junto com o *plone*. Mas antes de entrar em detalhe desse arquivo é necessário fazer uma cópia de segurança do **squid.conf** que seu *proxy* utiliza, pois vamos trocar esse arquivo pelo que está dentro da pasta **squid_direct**.

Entre na pasta onde o **squid.conf** *Default* está; e faça a cópia de segurança do arquivo.

```
cd /etc/squid
cp squid.conf squid.conf.bkp
```

Copie o **squid.conf** da pasta **squid_direct** para a pasta onde está o **squid.conf** *Default;* sobre escrevendo-o.

```
cp squid.conf /etc/squid/squid.conf
```

Copie para o mesmo diretório do **squid.conf** os arquivos **squidAcl.py**, **iRedirector.py** e **redirector_class.py**.

```
cp squidAcl.py /etc/squid/
cp iRedirector.py /etc/squid/
cp redirector_class.py /etc/squid/
```

Veja que a configuração *Default* do **CacheFu** está configurada para os pacotes Debian, caso não utilize o *squid* do *Debian* é necessário fazer algumas alterações nos 2 arquivos a seguir:

```
squidAcl.py
squid.conf
```

Pois estes arquivos farão referencias a arquivos que não estão localizados onde esses arquivos indicam, fazendo com que o *squid* não funcione. Exemplo com **squid.conf**.

```
external_acl_type    is_cacheable_type    children=20    %{Cookie:__ac}    %
{Cookie:;__ac} %{Authorization} %{If-None-Match} /etc/squid/squidAcl.py

redirect_program /etc/squid/iRedirector.py
```

Veja que essas duas linhas de comando do **squid.conf** tem referência a pasta */etc/squid* com seus respectivos arquivos, caso o *squid* não encontre os arquivos nos locais indicados ele não vai funcionar. Então é bom ter certeza onde os seus arquivos estão, para que o *squid* funcione. Outra observação seria com relação ao python que os *scripts* **iRedirector.py** e o **squidAcl.py** utilizam, pois as vezes dão problemas. Para evitar esse transtorno, indique no script o python que sua instância *zope* utiliza, trocando

```
/usr/bin/python -Ou
```

por

```
/home/nomedousuario/seupythoninstalado/bin/python -Ou
```

5) Samba

a) O que é

O Samba é um servidor que permite a comunicação entre máquinas *Windows* e Linux. Em nosso caso o samba proverá as estações baseadas em *Windows* a possibilidade de acesso aos arquivos salvos no servidor bem como a autenticação através do servidor Linux. Existem inúmeras funcionalidades que não serão abordadas aqui, e que vale uma pesquisa para possíveis implementações, já que buscamos aqui um texto simples e que permita a montagem/configuração rápida de um servidor de autenticação/arquivos em rede Linux/Windows.

b) Instalar

A instalação do SAMBA é via pacote; no terminal digite:

```
# apt-get install samba
```

c) Configurar

Uma vez instalado o pacote devemos editar o arquivo */etc/samba/smb.conf*. Já que no samba existem muitas opções, o que seria demasiadamente longo a explicação de todos, então será listado abaixo um *smb.conf.*

Para edita-lo:

```
$sudo gedit  /etc/samba/smb.conf
```

```
[Global]
log file = /var/log/samba/log.%m
smb passwd file = /etc/smbpasswd
admin users = administrador                     # Administrador do domínio
local master = yes
domain master = yes
domain logons = yes
#unix password sync = yes
null passwords = no
load printers = yes
name resolve order = host wins bcast
socket options = TCP_NODELAY SO_SNDBUF=8192 SO_RCVBUF=8192
hosts equiv = /etc/hosts
#hostname lookups = yes
username map = /etc/smbusers
encrypt passwords = yes
hosts allow = 10.3.131.0/24                     #
logon drive = c:
logon script = logon.bat
logon path = \\%L\profiles
logon home = \\%L\profiles
password level = 0
wins support = true
```

```
dns proxy = no
netbios name = samba
server string = Servidor de Arquivos PDC
remote announce = 10.3.131.0                                    #
workgroup = camara                                                    #
os level = 65
debug level = 1
printcap name = /etc/printcap
security = user
max log size = 100
domain logons = yes
domain logons = yes
#-----------------------------------SHARES--------------------------------#
[netlogon]
    writeable = yes
    path = /home/netlogon
    force create mode = 0777
    create mask = 0777
    comment = Network Logon Service
    public = yes

[profiles]
    comment = %u
    path = /home/%u
    public = yes
    writable = yes
    browseable = yes
    printable = no
    create mask = 0777
    force create mode = 0777

[home]
    comment = Home
    path = /home
    public = yes
    writable = yes
    browseable = yes
    printable = no
    create mask = 0777
    force create mode = 0777

[usuarios]
    comment = Arquivos Pessoais
    path = /home/usuarios/%u
    public = no
    writable = yes
    browseable = yes
    printable = no
    create mask = 0777
    force create mode = 0777

[grupos]
    comment = Pasta do grupo
    path = /home/grupos/%g
    public = no
    writable = yes
    browseable = yes
    printable = no
    create mask = 0777
    force create mode = 0777

[Publico]
    path = /home/publico
    public = yes
    writable = yes
    browseable = yes
    printable = no
    create mask = 0777
    force create mode = 0777
    force directory mode = 0777
```

O arquivo listado acima é um exemplo de arquivo utilizado em uma Câmara do município de Timóteo – MG; e nele estão mapeados a estrutura de rede com as pastas:

```
• /home/<usuário>
• /home/usuarios/<usuário>
• /home/grupos/<grupo>
• /home/publico
```

Para o mapeamento das pastas no *Windows,* criamos o script[41] *logon.bat* em */home/netlogon* com o seguinte conteúdo:

```
net use k: \\samba\usuarios
net use l: \\samba\grupos
net use m: \\samba\Publico
```

6) DHCP (Dhcp server)

a) O que é

O Protocolo de Configuração Dinâmica de Hosts (DHCP) é um serviço de rede que permite que os computadores sejam configurados automaticamente a partir de configurações feitas em um servidor ao invés de serem configurados individualmente de forma manual. Computadores configurados para serem clientes de DHCP não tem controle sobre as configurações que eles recebem do servidor DHCP, e a configuração é transparente para o usuário do computador.

b) Instalar

Em um terminal, digite o seguinte comando para instalar **dhcpd**:

```
sudo apt-get install dhcpd
```

Você verá a seguinte saída, a qual explica o que fazer em seguida:

```
Por favor note que se você estiver instalando o servidor DHCP pela primeira
vez você irá precisar configurá-lo. Por favor pare (/etc/init.d/dhcp
stop) o serviço do servidor DHCP, edite o /etc/dhcpd.conf para
ajustá-lo às suas necessidades
e configurações particulares, e reinicie o serviço do servidor DHCP
(/etc/init.d/dhcp start).

Você também precisará editar o /etc/default/dhcp para especificar as interfaces que o dhcpd
deverá ouvir. Por padrão ele ouve na eth0.

NOTA: as mensagens do dhcpd são enviadas para o syslog. Procure lá por
mensagens de diagnóstico.

Iniciando o servidor DHCP: o dhcpd falhou ao iniciar - verifique o syslog para diagnosticar o
problema.
```

c) Configuração

A mensagem de erro encontrada no final da instalação pode ser um pouco confusa, mas os seguintes passos vão te ajudar a configurar o servidor:

Geralmente, o que você quer fazer é associar um endereço IP de forma aleatória. Isto pode ser feito com as seguintes configurações:

41 Script: Descrição de uma tarefa complexa ou de uma série de tarefas usando uma linguagem de programação.

```
# Exemplo /etc/dhcpd.conf
# (adicione seus comentários aqui)
default-lease-time 600;
max-lease-time 7200;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.1.255;
option routers 192.168.1.254;
option domain-name-servers 192.168.1.1, 192.168.1.2;
option domain-name "mydomain.org";

subnet 192.168.1.0 netmask 255.255.255.0 {
range 192.168.1.10 192.168.1.100;
range 192.168.1.150 192.168.1.200;
}
```

Isso irá fazer com que o servidor DHCP atribua ao cliente um endereço IP a partir da faixa 192.168.1.10-192.168.1.100 ou 192.168.1.150-192.168.1.200. Ele irá emprestar um endereço por 600 segundos se o cliente não perguntar por um determinado período de tempo. O servidor também irá "avisar" o cliente que ele deve usar 255.255.255.0 como sua máscara de sub-rede, 192.168.1.255 como seu endereço de *broadcast*[42], 192.168.1.254 como roteador/gateway e 192.168.1.1 e 192.168.1.2 como seus servidores DNS.

Se for preciso especificar um servidor WINS para os seus clientes de *Windows*, você deverá incluir a opção netbios-nome-servidor.

```
option netbios-name-servers 192.168.1.1;
```

Configurações do *dhcpd* foram adquiridas do *mini-HOWTO do DHCP*, que pode ser encontrado no link http://www.tldp.org/HOWTO/DHCP/index.html

7) Backup

Backup refere-se à cópia de dados de um dispositivo para o outro com o objetivo de posteriormente recuperá-los. Para isso precisamos saber aonde ficam os dados, veja a seguir o caminho da base de dados de cada sistema.

Todas essas informações se baseiam que a instalação dos produtos foram realizadas nas pastas recomendadas na instalação.

a) Aonde fica os dados para backup?

Zope

#Caminho da base de dados do SAPL

```
/var/lib/zope2.8/instance/sapl/var
```

#Caminho da base de dados do Portal Modelo

```
/var/lib/zope2.8/instance/portalcasas/var
```

#Caminho da base de sados do SAAP

42 Broadcast: Uma transmissão enviada a mais de um receptor

```
/opt/saap/zope/var
```

SAPL

O cadastro de usuários:

```
/var/lib/zope2.8/instance/sapl/var/Data.fs
```

Textos integrais de matérias, proposições ou normas jurídicas:

```
/var/lib/zope2.8/instance/sapl/var/DocumentosSapl.fs
```

No MySQL, ficam todos os dados do sistema:

```
/var/lib/mysql/interlegis
```

Portal Modelo

Base de dados

```
/var/lib/zope2.8/instance/portalcasas/Data.fs
```

Se você utiliza vídeos ou arquivos armazenados no sistema de arquivos faça backup do diretório '/var/lib/zope2.8/instance/portalcasas/var' inteiro pois é lá que esses arquivos serão armazenados

Se você atualizou ou instalou algum **produto** novo faça backup[43] também do diretório '/var/lib/zope2.8/instance/portalcasas/Products'.

SAAP

Arquivos de dados

```
/opt/saap/zope/var/Data.fs
```

8) Conexão remota via SSH

a) O que é

E um protocolo Secure Shell (SSH), serve para controlar um computador remotamente ou transferir arquivos entre computadores.

b) Instalar

Para utilizar este protocolo usaremos como base uma poderosas ferramentas para o controle remoto de computadores ligados em rede e transferência de dados entre computadores na rede, chamado *OpenSSH*.

Para instalar o OpenSSH cliente no seu Ubuntu, use este comando no terminal:

43 Backup refere-se à cópia de dados de um dispositivo para o outro com o objetivo de posteriormente recuperá-los

```
sudo apt-get install openssh-client
```

Para instalar o OpenSSH servidor no seu Ubuntu, use este comando no terminal:

```
sudo apt-get install openssh-server
```

c) Configurar

Você pode configurar o comportamento padrão do servidor OpenSSH, **sshd**, editando o arquivo `/etc/ssh/sshd_config`. Para mais informação sobre as diretrizes de configuração usadas neste arquivo, você pode ver o manual apropriado com o seguinte comando, executado pela linha de comando:

```
man sshd_config
```

Capítulo 9 - Estação do cliente (suporte ao usuário linux)

Todas as informação abaixo se referem a versão do Ubuntu 8.04 (Hardy Heron).

Para que o usuário final tenha sucesso na utilização de suas tarefas, o sistema operacional deve ser dotado de algumas ferramentas para auxiliar no trabalho:

1) Internet

a) E-mail

Para receber e enviar e-mail utilizaremos a ferramenta *Thunderbird.*

Para instalar

```
sudo apt-get install thunderbird
```

Criando uma conta nova no Thunderbird

Agora abra o Thunderbird e crie uma conta através do menu `Ferramentas > Configurar contas`. Clique no botão `Nova conta`.

- Selecione `Conta de email` e clique em `Avançar`.
- Preencha o seu nome e o email @servidor.com.br e clique em `Avançar`.
- Selecione `POP`.
- No campo `Receber mensagens por este servidor` coloque `pop.servidor.com.br`.
- Se houver o campo `Enviar mensagens por este servidor SMTP`, preencha com `smtp.servidor.com.br`.
- Clique em `Avançar`.
- Em `Nome de usuário` preencha o seu email. Exemplo: `a.lima@brturbo.com.br`.
- Se houver o campo `Nome de usuário do servidor SMTP`, repita o mesmo email do passo anterior.
- Clique em `Avançar`.
- Em `Nome da conta` preencha um nome qualquer. Exemplo: `Conta do BrTurbo`.
- Clique em `Avançar` e `Concluir`.

Agora é necessário configurar a conta recém-criada para que utilize conexões criptografadas.

- Ainda na janela `Configurar contas`, clique no painel `Servidor` da conta do servidor, no exemplo “BrTurbo”.
- Marque a opção `Usar conexão segura: SSL`. O campo `Porta` deve ser `995`.
- Deixe **desmarcada** a opção `Usar autenticação segura`.

Enviando mensagens (servidor SMTP)

Com a conta POP configurada já é possível receber emails. Continue para configurar o envio de mensagens.

- Na janela `Configurar contas`, clique em `Servidor de envio (SMTP)` no painel à esquerda (o último item).
- Clique em `Adicionar`.
- No campo `Descrição` preencha `BrTurbo` (ou qualquer outra descrição).
- No campo `Servidor` preencha `smtp.servidor.com.br`.
- No campo `Porta` coloque `587`.
- Marque a opção `O servidor requer autenticação`.
- Preencha `Nome de usuário` com o seu email. Exemplo: `a.lima@brturbo.com.br`.
- Em `Usar conexão segura`, selecione `TLS` (verifique se o campo `Porta` continua `587`).
- Clique em `OK`.

Agora você deve associar o novo servidor SMTP à conta sua conta:

- Selecione, no painel a esquerda, o item principal da conta .
- Aparecerá a tela com sua identidade padrão (seu nome e email).
- Na opção `Servidor de envio (SMTP)`, selecione o servidor que você acabou de adicionar.

Está pronto. Agora clique em `OK` para fechar a janela. Clique no botão `Receber` e baixe suas mensagens.

Caso o Thunderbird não consiga se conectar verifique se algum programa firewall ou antivírus está impedindo a conexão para as portas 587 e 995.

b) Navegador Web

Para navegação na Internet, utilizaremos o navegador que já vem por padrão no sistema, o *Mozilla Firefox*. Um navegador padrão com as seguintes vantagens:

- Abas: várias páginas dentro de uma janela
- Extensões: adicione novas funcionalidades ao Firefox
- Indicações de segurança
- Busca de texto na página em instantes
- Navegação mais segura com a proteção contra fraude
- Temas: modifique a visual com novos ícones e cores
- Bloqueador de janelas popup
- Campo de pesquisa

Mais detalhes sobre o navegados podem ser encontrados no link http://br.mozdev.org/firefox/vocesabia/#dicas-a

c) Mensageiro eletrônico

Utilizaremos para este fim o Gajim, é um pequeno cliente de jabber, que , para quem não sabe, é um protocolo de mensagens instantâneas, como o msn, mas de código aberto.

Instalar

Para instalar digite no terminal:

```
apt-get install gajim
```

Configurar

Para configurar uma conta de menssageiro abra o gajim e automaticamente surge a opção de criar nova conta. Escolha que já tenho uma conta e quero usa-la. Depois de avançar, coloco o nome de utilizador, que é a primeira parte do e-mail, por exemplo, "utilizador_de_email" e logo de seguida o servidor. Introduzo a senha e clico em avançar. Em vez de premir terminar escolho avançado, vou até ao separador ligação e escolho utilizar hostname/porta personalizados, que por exemplo o mensageiro *Sapo* é o clientes.im.sapo.pt. Clique em *gravar* e já está ok. É só colocar disponível.

Para falar com os amigos do msn, clico em ações >> descobrir recursos >> e logo surgem os *transports* disponíveis basta escolher o msn por exemplo e clicar em registrar. Vai então ser solicitado o endereço e senha do msn.

2) Pacote de escritório

OpenOffice.org é uma suíte de aplicativos para escritório livres multiplataforma. A suíte[44] usa o formato ODF (OpenDocument) e é compatível com o formato de outras ferramentas, por exemplo o *Microsoft Office.*

Ele já vem instalado por padrão no Ubuntu e pode ser acessado pelo >> menu de navegação superior >> Aplicações >> Escritório, o sistema retorna uma lista com as ferramentas de:

- Editor de Textos;
- Planilha de cálculos;
- Apresentação (Slides).

3) Multimídia

Instalar Codecs[45]

Abrir o terminal e escrever:

```
sudo -s -H
```

ou

```
sudo -i
```

e por a senha do utilizador.

Depois disso:

```
apt-get update
```

44 Suíte: conglomerado de aplicativos com um fim especifico.

45 **Codec:** Softwares que auxiliam o sistema operacional a executar determinados tipos de arquivos. Ex.: músicas mp3.

```
apt-get upgrade
```

Para ficar atualizado. **Por favor verifica se todos os repositórios estão ativos nas fontes de software.**

Depois estes comandos:

```
apt-get install gstreamer0.10-plugins-ugly-multiverse gstreamer0.10-plugins-bad-multiverse
gstreamer0.10-plugins-bad gstreamer0.10-plugins-ugly gstreamer0.10-ffmpeg libxine1-ffmpeg
libdvdread3
```

Agora tens a maioria dos *codecs* que necessitas para a maioria dos formatos multimídia.

Instalar suporte DVD

No terminal digite:

```
sudo gedit /etc/apt/sources.list
```

Copie os dados abaixo (ctrl+c) e cole (ctrl+v) no arquivo aberto:

```
## Medibuntu - Ubuntu 8.04 "hardy"
## Please report any bug on https://bugs.launchpad.net/medibuntu/
deb http://packages.medibuntu.org/ hardy free non-free
```

Salve o documento e digite no terminal:

```
wget -q http://packages.medibuntu.org/medibuntu-key.gpg -O- | sudo apt-key
add -
```

Finalmente digite no terminal:

```
sudo apt-get update

sudo apt-get install libdvdcss2
```

Referência

http://ubuntupedia.info/index.php/P%C3%A1gina_principal

https://help.ubuntu.com/6.06/ubuntu/serverguide/pt_BR/introduction-chap.html

http://pt.wikipedia.org/

http://colab.interlegis.gov.br/wiki

TUTORIAL DNS

http://www.inf.ufsc.br/~ine5384-hp/Hashing/

http://listas.interlegis.gov.br/pipermail/gitec/

http://www.tldp.org/HOWTO/DHCP/index.html

http://www.linuxman.pro.br/node/1

http://plone.org/products/cachefu

http://br-linux.org/2008/migracao-para-software-livre-na-camara-de-timoteo/

Glossário