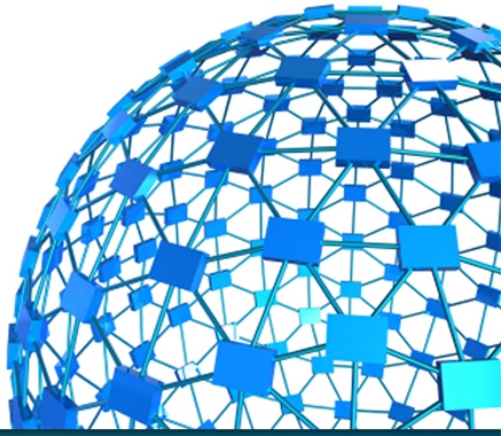
FORMAÇÃO GESAC

KIT SOS
REDE LOCAL



Comentários dos autores

Não tenha receio de aprender coisas novas, pois a vida é uma escola.
Algumas ilustrações apresentadas são apenas arte representativa. Qualquer semelhança com a realidade é mera coincidência.

PRESIDÊNCIA DA REPÚBLICA

Luiz Inácio Lula da Silva
Presidente da República

MINISTÉRIO DAS COMUNICAÇÕES

José Artur Filardi Leite
Ministro de Estado das Comunicações

Secretaria Executiva

Fernando Rodrigues Lopes de Oliveira
Secretário Executivo

Secretaria de Telecomunicações

Roberto Pinto Martins
Secretário

Departamento de Serviços de Inclusão Digital

Heliomar Medeiros de Lima
Diretor

Elias Nagib David
Coordenador Geral do Projeto Formação Gesac

MINISTÉRIO DAS COMUNICAÇÕES
Secretaria de Telecomunicações
Departamento de Serviços de Inclusão Digital
Programa Gesac
Projeto Formação Gesac

KIT SOS GESAC

Rede Local

William da Silva Vianna
Ronaldo Amaral Santos
Organizadores

Brasília, DF
2010

1ª Edição – 2010

Realização
Ministério das Comunicações

Parceiros
Ministério da Educação
Conselho Nacional de Desenvolvimento Científico e Tecnológico
Rede Federal de Educação Profissional e Tecnológica

Organização
William da Silva Vianna
Ronaldo Amaral Santos

Conteudistas
Ewerton Lyrio Nascimento
Filipe Ribeiro Viana de Almeida
Wesley Folly Volotão de Souza

Arte da Capa
Pedro Henrique Parreiras de Meireles

Projeto Gráfico e Diagramação
Pedro Henrique Parreiras de Meireles

Revisão

Elias Nagib David
Janei Cristina Santos Resende
Maria da Graça Miranda da Silva

Sobre o Projeto
Esplanada dos Ministérios, Bloco L, Anexo I, sala 207
CEP: 70.047-900, Brasília – DF
Fone: (61) 2022-8686 / 8687
http://www.formacao.gesac.gov.br

Projeto Formação Gesac

KIT SOS Gesac – Rede Local. William da Silva Vianna e Ronaldo Amaral Santos. 1. ed. - Brasília: Ministério das Comunicações, 2010; [Campos dos Goytacazes]: Instituto Federal de Educação, Ciência e Tecnologia Fluminense.
29p. il. Color. , 27 cm

1. Inclusão Digital 2. Ubuntu 3. Windows. I. Brasil. Ministério das Comunicações. II. Instituto Federal de Educação, Ciência e Tecnologia Fluminense. III. Título.

CDU 37:004

Sumário

Lista de siglas e abreviação

- kbps – kilo bits por segundo;
- kilo – mil;
- WAN - Wide Area Network – rede de longa distância;
- WEB ou WWW - World Wide Web é um sistema hipertexto que funciona sobre a Internet. A visualização da informação e navegação é feita usando uma aplicação específica - o navegador (browser);
- MSN - Microsoft Service Network;
- ICQ - é um programa de comunicação instantânea pela Internet que pertence à companhia América Online;
- plugins - também conhecido por plug-in, add-in, add-on. É um programa de computador usado para adicionar funções a outros programas maiores, provendo alguma funcionalidade especial ou muito específica;

1. Introdução

O Projeto Formação Gesac está inserido no Programa de inclusão digital Gesac, desenvolvido pelo Ministério das Comunicações, que leva Internet em banda larga a mais de 11 mil telecentros em todo o País. Com duração inicial de um ano, o Projeto capacitará até abril de 2011, monitores e multiplicadores de 739 Pontos Gesac em Tecnologias de Informação e Comunicação (TICs).

O objetivo é transformar a realidade dessas comunidades ao apresentar seus integrantes a esse novo universo, oferecendo, além de internet banda larga, conhecimento nas TICs, possibilitando assim a construção de alternativas reais de interação com autonomia nas redes digitais. A ação é realizada por meio de parceria com o Ministério da Educação, com o a Rede Federal de Educação Profissional e Tecnológica e o Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq).

Ao acessar esses instrumentos, os atores podem conquistar a autonomia para encontrar seus próprios caminhos de desenvolvimento, coerentes com sua cultura e objetivos. Esse resultado esperado do projeto é fundamental para o exercício da cidadania, pois leva informação e possibilidade de interação com outras esferas da sociedade, possibilitando desenvolvimento social e econômico nas localidades alcançadas.

Os 739 Pontos Gesac inicialmente atendidos neste projeto, em sua grande maioria, possuem acesso a Internet com link de 256 kbps provido por link de satélite. A tecnologia que provê acesso a Internet por satélite possui algumas limitações, entre elas está a alta latência (tempo de reposta). Satélites são usados em muitas partes do mundo para suprir linhas terrestres indisponíveis ou caras. Apesar de ser possível obter a um custo razoável uma largura de banda significativa para um link baseado em satélite, a distância em relação à Terra causa uma grande latência. Para efeito de comparação, o tempo de ida e volta em link WAN (Wide Area Network) transoceânico ou que cruze um continente costuma ficar entre 100 e 200 ms (milissegundos), enquanto o link de um satélite pode facilmente demorar até dois segundo. Esse enorme tempo acarreta atrasos importantes, especialmente em protocolos de aplicativo como o navegador de Internet (Firefox, Opera, Chrome, Internet Explorer, etc). A figura 1 ilustra o link de satélite permitindo que o PC (computador) em locais distantes possa fazer uso da Internet.

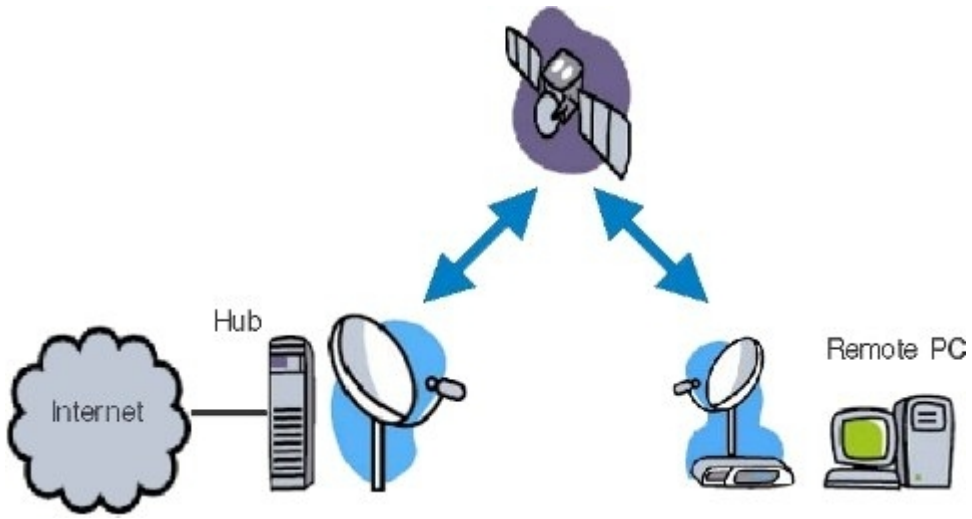


Ilustração 1: Link de Internet por satélite

Como se a latência não fosse o suficiente para degradar o desempenho, ainda podem existir máquinas na rede local do ponto Gesac realizando operações indevidas que aumentam o uso do link sem o usuário ter conhecimento. Estas operações indevidas e não solicitadas são geradas pelo sistema operacional e, em muitos casos, por softwares maliciosos como: vírus, worm, cavalos de tróia, bot de spam, bot de phishing, keylog, screenlog, etc. As recomendações para melhorar o desempenho do acesso a Internet das estações Windows podem ser obtidas no arquivo **kitsos_windows**.

1.1. Objetivos

O presente documento propõe a aumento do desempenho da rede local a partir da configuração de proxy e filtragens. Considerando este contexto, este documento tem como objetivo:

1 – Explanar sobre a segurança da informação e sua relação com o desempenho;

2 - Propor soluções práticas e recomendações para aumentar o desempenho da rede local dos pontos Gesac;

A proposta de uso de sistema de cache (proxy) e filtros apenas visa melhorar o desempenho de acesso a Internet. Se o acesso é o seu acesso provido por link de satélite então existem limitações físicas e tecnológicas que impedirão uma melhora significativa, ou seja, neste caso não existe milagre. Esta solução se aplica nos pontos Gesac sem qualquer tipo de solução já implementada. Não recomendamos a substituição da solução Metasys Server.

1.2. Pré-requisitos

Os pré-requisitos para implementação da solução com sucesso depende das noções básicas de redes e serviços de redes. Entretanto, este documento foi criado para permitir a implementação da solução por pessoas com muito pouco conhecimento sobre o assunto. Para tal, as configurações básicas estão armazenadas no DVD, bastando apenas a recuperação do backup que será explicado mais adiante. Além disso, é necessário um microcomputador com duas interfaces de rede. Este microcomputador poderá operar sem teclado, mouse e monitor. A configuração mínima do hardware para até 25 clientes deve ser;

- Pentium 3 de 1GHz ou equivalente;

- 512MB de memória RAM;

- disco rígido de 8 GB;

- 2 interfaces de rede PCI;

Para melhor entendimento da solução, este documento explana sobre alguns conceitos de redes e recomendações.

2. Noções dos protocolos TCP, UDP, ICMP e IP

Antes de iniciar a leitura deste tópico, recomendo assistir ao vídeo **warriors_of_the_net.avi** localizado no diretório **vídeos**. Trata-se de uma animação 3D que explica de forma simples o funcionamentos de alguns protocolos e recursos utilizados na Internet.

2.1. IP – Internet Protocol

O endereço IP (Internet Protocol), de forma genérica, é um endereço que indica o local de um determinado equipamento (normalmente computadores) em uma rede privada ou pública.

Para um melhor uso dos endereços de equipamentos em rede pelas pessoas, utiliza-se a forma de endereços de domínio, tal como "www.wikipedia.org". Cada endereço de domínio é convertido em um endereço IP pelo DNS. Este processo de conversão é conhecido como resolução de nomes de domínio.

Os dados numa rede IP são enviados em blocos referidos como pacotes (os termos são basicamente sinônimos no IP, sendo usados para os dados em diferentes locais nas camadas IP). Em particular, no IP nenhuma definição é necessária antes de uma máquina tentar enviar pacotes para

um outra máquina com o qual não comunicou previamente.

O IP oferece um serviço de datagramas não confiável (também chamado de melhor esforço); ou seja, o pacote vem quase sem garantias. O pacote pode chegar desordenado (comparado com outros pacotes enviados entre os mesmos nós), também podem chegar duplicados, ou podem ser perdidos por inteiro. Se a aplicação requer maior confiabilidade, esta é adicionada na camada de transporte.

Os roteadores são usados para reencaminhar datagramas IP através das redes interconectadas na segunda camada. A falta de qualquer garantia de entrega significa que o desenho da troca de pacotes é feito de forma mais simplificada. (Note que se a rede cai, reordena ou de outra forma danifica um grande número de pacotes, o desempenho observado pelo utilizador será pobre, logo a maioria dos elementos de rede tentam arduamente não fazer este tipo de coisas - melhor esforço. Contudo, um erro ocasional não irá produzir nenhum efeito notável.)

O IP é o elemento comum encontrado na Internet pública dos dias de hoje. É descrito no RFC 791 da IETF, que foi pela primeira vez publicado em Setembro de 1981. Este documento descreve o protocolo da camada de rede mais popular e atualmente em uso. Esta versão do protocolo é designada de versão 4, ou IPv4. O IPv6 tem endereçamento de origem e destino de 128 bits, oferecendo mais endereçamentos que os 32 bits do Ipv4.

O endereçamento IP na versão IPv4 possui 4 números de 0 a 255 separados por um ponto (exemplo: 192.168.0.1). Além disso, existe o uso de outro endereço chamado de máscara de rede. Este endereço define quantos são os endereços IPs disponíveis em uma rede e qual a sua faixa. Exemplo: rede 192.168.0.0 mascara: 255.255.255.0 possui endereços disponíveis para as máquina entre 192.168.0.1 e 192.168.0.254

2.2. TCP – Protocolo de Controle de Transmissão

O TCP (acrônimo para o inglês Transmission Control Protocol) é um dos protocolos sob os quais assenta o núcleo da Internet. A versatilidade e robustez deste protocolo tornou-o adequado a redes globais, já que este verifica se os dados são enviados de forma correta, na sequência apropriada e sem erros, pela rede.

O TCP é um protocolo do nível da camada de transporte (camada 4) do Modelo OSI e é sobre o qual assentam a maioria das aplicações cibernéticas, como o SSH, FTP, HTTP — portanto, a World Wide Web.

2.3. UDP - User Datagram Protocol

É um protocolo que permite a comunicação entre computadores diferentes. É uma comunicação sem conexão que não garante de a chegada dos pacotes em ordem particular, diferente do TCP.

2.4. ICMP – Protocolo de Internet para Controle de Mensagem

ICMP, sigla para o inglês Internet Control Message Protocol, é um protocolo integrante do Protocolo IP e utilizado para fornecer relatórios de erros à fonte original. Geralmente, os computador que utilize IP aceitam as mensagens ICMP e alteram o seu comportamento de acordo com o erro relatado. Os gateways devem estar programados para enviar mensagens ICMP quando receberem datagramas que provoquem algum erro.

As mensagens ICMP geralmente são enviadas automaticamente em uma das seguintes situações:

- Um pacote IP não consegue chegar ao seu destino (i.e. Tempo de vida do pacote expirado);

- O Gateway não consegue retransmitir os pacotes na frequência adequada (i.e. Gateway congestionado);

- O Roteador ou Encaminhador indica uma rota melhor para a máquina a enviar pacotes.

Ferramentas comumente usadas em Windows baseadas nesse protocolo são: Ping e Traceroute.

3. Conceitos de serviços

3.1. Surgimento do servidor proxy

O servidor proxy surgiu da necessidade de conectar uma rede local à Internet através de um computador da rede que compartilha sua conexão com as demais máquinas. Ou seja, se considerarmos que a rede local é uma rede "interna" e a Internet é uma rede "externa", podemos dizer que o proxy é que permite outras máquinas terem acesso externo.

Geralmente, máquinas da rede interna não possuem endereços válidos na Internet e, portanto, não têm uma conexão direta com a Internet. Assim, toda solicitação de conexão de uma máquina da rede local para um host da Internet é direcionada ao proxy, este, por sua vez, realiza o contato com o host desejado, repassando a resposta à solicitação para a máquina da rede local. Por este motivo, é utilizado o termo proxy para este tipo de serviço, que é traduzido para procurador ou intermediário.

É comum termos o proxy com conexão direta com a Internet.

Uma aplicação proxy popular é o caching web proxy, um web proxy usado com cache. Este provê um cache de páginas da Internet e arquivos disponíveis em servidores remotos da Internet, permitindo aos clientes de uma rede local (LAN) acessá-los mais rapidamente e de forma viável.

3.2. Proxy WEB

Um HTTP caching proxy ou proxy WEB, permite que o cliente requisite um documento na World Wide Web e o proxy procura pelo documento em seu cache. Se encontrado, o documento é retornado imediatamente. Caso contrário, o proxy busca o documento no servidor remoto, entrega-o ao cliente e salva uma cópia no seu cache. Isso permite uma diminuição na latência, já que o servidor proxy, e não o servidor original, é acessado, proporcionando ainda uma redução do uso de banda. No caso dos pontos Gesac com acesso por satélite este tipo de recurso é fundamental para um melhor desempenho. A ilustração 2 apresenta o esquema básico de uma rede com proxy WEB.

Ilustração 2: Esquema básico de um proxy WEB

Quando o servidor proxy WEB recebe uma solicitação para aceder a um recurso da Internet (especificado por uma URL), um proxy que usa cache procura por resultados desta URL no seu cache local. Se o recurso for encontrado, ele é retornado imediatamente. Senão, ele carrega o recurso do servidor remoto, retornando-o ao solicitador e armazena uma cópia deste no seu cache. O cache usa normalmente um algoritmo de expiração para a remoção de documentos de acordo com

a sua idade, tamanho e histórico de acesso.

O proxy também é usado para navegar anonimamente, ou seja, é feita a substituição de um proxy por outro, afim de burlar proteções oferecidas pelo proxy original.

A privacidade de servidores de proxy públicos é questionável, pois existem indícios que certos proxys anônimos geram logs com dados reais de seus usuários. Além disso, muitos proxys anônimos implantam softwares maliciosos (malware) nos clientes que o acessam.

3.2.1. Transparência

Um proxy transparente é um método para obrigar os utilizadores de uma rede a utilizarem o proxy. Além das características de caching dos proxies convencionais, estes podem impor políticas de utilização ou recolher dados estatísticos, entre outras. A transparência é conseguida interceptando o tráfego HTTP (por exemplo) e reencaminhando-o para o proxy mediante a técnica ou variação de port forwarding. Assim, independentemente das configurações explícitas do utilizador, a sua utilização estará sempre condicionada às políticas de utilização da rede.

3.3. Firewall

Firewall (em português: muro corta-fogo) é o nome dado ao 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 a uma parede corta-fogo (firewall), que evita o alastramento de incêndios pelos cômodos de uma edificação.

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.

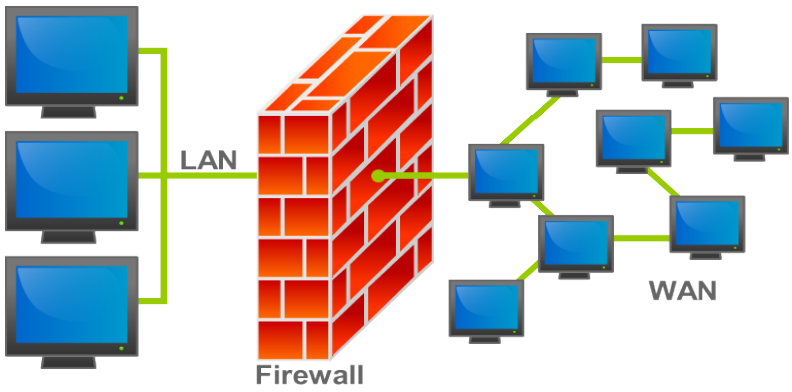


Ilustração 3: Ilustração de um firewall entre a rede local (LAN) e a Internet (WAN)

Faremos uso de firewall implementado por software devido a facilidade de implementação e custo. Existem muitas distribuições GNU/Linux que se destinam exclusivamente para serviços de rede como firewall. A seguinte url apresenta algumas destas distribuições:

http://distrowatch.com/search.php?category=Firewall#distrosearch

Após análise comparativa em mais de 20 distribuições Linux específicas para Firewall, Endian Firwall foi selecionada como a mais adequada para uso nos pontos Gesac que não possuem solução de proxy e filtragem já implementada.

Endian Firewall é um projeto open source baseado no conhecido IPCop, desenvolvido pela ENDIAN, empresa italiana de gerenciamento e segurança de redes. Com a instalação do Endian Firewall, suprimos basicamente todas as necessidades de uma rede, como Firewall, IDS, Proxy, Servidor DHCP, Servidor NTP, antivírus, fitro de conteúdo, Controle de Tráfego, etc. Esta distribuição (Endian Firewall) necessita de um microcomputador dedicado para estes serviços, ou seja, este microcomputador não poderá ser utilizado com estação de trabalho. Entretanto, este microcomputador não precisa ser de última geração, pelo contrário, o requisito mínimo para atender até 20 clientes é um Pentium III (ou equivalente) com 256 MB de RAM, 2 placas de rede e 8 GB de disco rígido.

4. Endian Firewall

4.1. Recursos interessantes e relevantes

* Interface WEB limpa, rápida, e intuitiva para administração;

4.1.1. Firewall:

* Até 4 redes diferentes, separadas pelo sistema de cores Green (rede local), Red (WAN), Orange (DMZ), Blue (Wireless)

Ilustração 4: Esquema de cores para as redes do Endian Firewall

* Firewall baseado em iptables, gerenciamento simples e eficiente, tanto para saída, como entrada e entre redes diferentes, garantindo um plus na segurança.

* NAT, SNAT, DNAT, “port forward”, de forma intuitiva e simples

4.1.2. Segurança Web:

* proxy transparente para FTP

* Antivirus para sites e arquivos baixados

* bloqueios e filtros de arquivos

* blacklists prontas para diversas categorias

* Dansguardian para controle de conteúdo mais eficiente (pegando o que as blacklists não pegaram)

* Proxy transparente (squid)

* Proxy autenticado (squid) (local, ldap, radius, Active Directory)

* Controle de acesso por horário (bloqueia sites “não profissionais” durante o horário de trabalho e libera a noite)

* Controle de acesso por grupos

4.2.3. Segurança de E-mails:

* Anti-Spam com Bayes e registros SPF

* Proxy transparente para pop3, imap e smtp

* Black/White Lists

* Mail forward transparente (bcc)

VPN (virtual private network)

* OpenVPN e IPSec

* autenticação por usuário/senha e/ou por chaves.

* Simples e sem mistério, precisando apenas de 3 ou 4 cliques

* VPN entre duas redes remotas, interligando escritórios, ou entre um cliente (roadwarrior) e o servidor.

* “Push” de rotas e requests de dns.

Multi-Wan Com failover

* Suporta ligar dois ou mais links de operadoras diferentes, caso o link primário fique fora do ar, automagicamente passa para o link de reserva.

4.1.4. Logs, estatísticas, IDS e relatórios

* IDS (Snort) integrado

* ntop para estatísticas detalhadas de tráfego.

* estatísticas e gráficos de tráfego de cada interface (rede), sistema (cpu, memoria, etc), envio e recebimento de emails, pageviews e estatísticas obtidas do squid.

* logs via web do squid, dansguardian, firewall, postfix, clamAV

* Syslog local e remoto

4.1.5. Backup e gerenciamento

* Backup e restauração via web, em teoria possibilitando “clonar” rapidamente o servidor principal em caso de pane da máquina. (Ou em caso de “mancada administrativa”)

* Gerenciamento via SSH, Console e Web usando SSL.

4.2. Instalação do Endian Firewall

4.2.1. Instalação do sistema operacional

A instalação é simples e pode ser executada conforme o procedimento descrito no arquivo "**instalacao_EndianFirewall**" que se encontram na pasta **doc**. A ISO para gravação do CD de instalação da versão 2.4 encontra-se no diretório softwares (**EFW-COMMUNITY-2.4-201005280528-RESPIN.iso**).

4.2.2. Instalação do firewall na rede local

A máquina, que agora será o firewall da rede, precisa ser ligada entre a rede local e o equipamento que promove a acesso a Internet utilizando a antena do ponto Gesac.

O esquema será o seguinte:

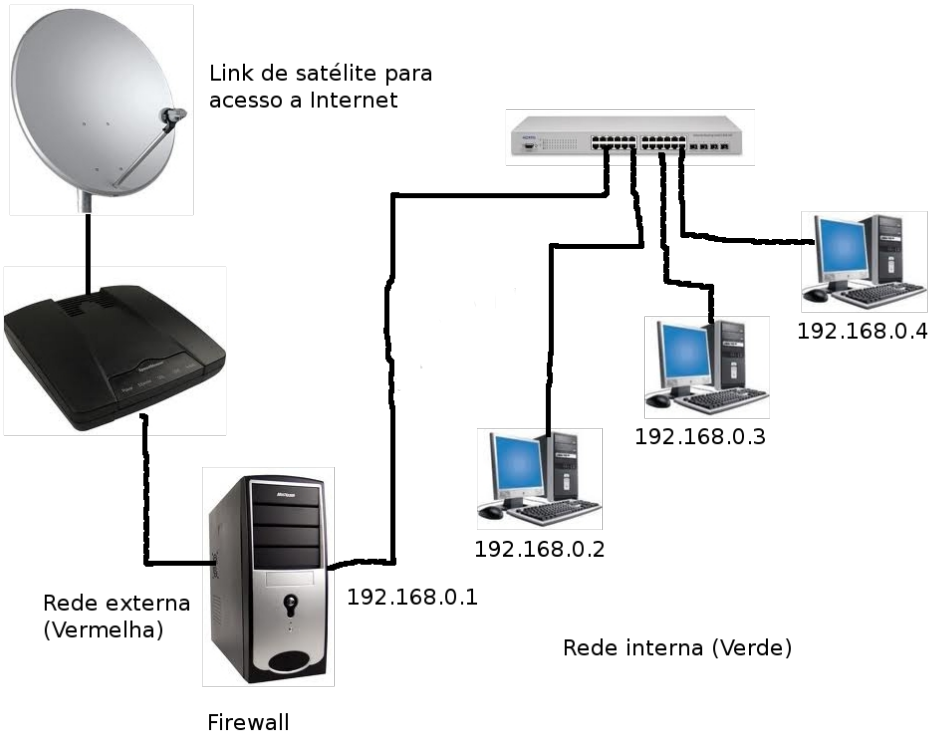


Ilustração 5: Diagrama da rede com uso do Firewall

As máquinas localizada na rede interna não precisam ter endereço IP configurado manualmente, basta ativar o DHCP automático para que o firewall atribua um endereço IP da rede interna. A partir

deste momento poderá ser realizado o acesso inicial ao firewall.

4.3. Acesso inicial ao Endian Firewall

Com o microcomputador conectado a rede local conforme diagrama da figura 5, execute o navegador de Internet (Mozilla Firefox) e digite na barra de endereço:

https://192.168.0.1:10443

Caso este seja o endereço IP atribuído ao firewall durante a instalação, caso não, utilize o endereço que você definiu. Deverá surgir uma janela conforme a apresentada na figura seguinte.

O acesso realizado na interface WEB de administração é encriptado, logo será fornecida uma chave de encriptação que deverá ser aceita.

Ilustração 6: Chave de criptografia para acesso encriptado

Clique em “Adicionar exceção...” e aceite a chave de encriptação.

Após surgirá a página de boas vindas do Endian Firewall. Clique no botão “>>>” para prosseguir.

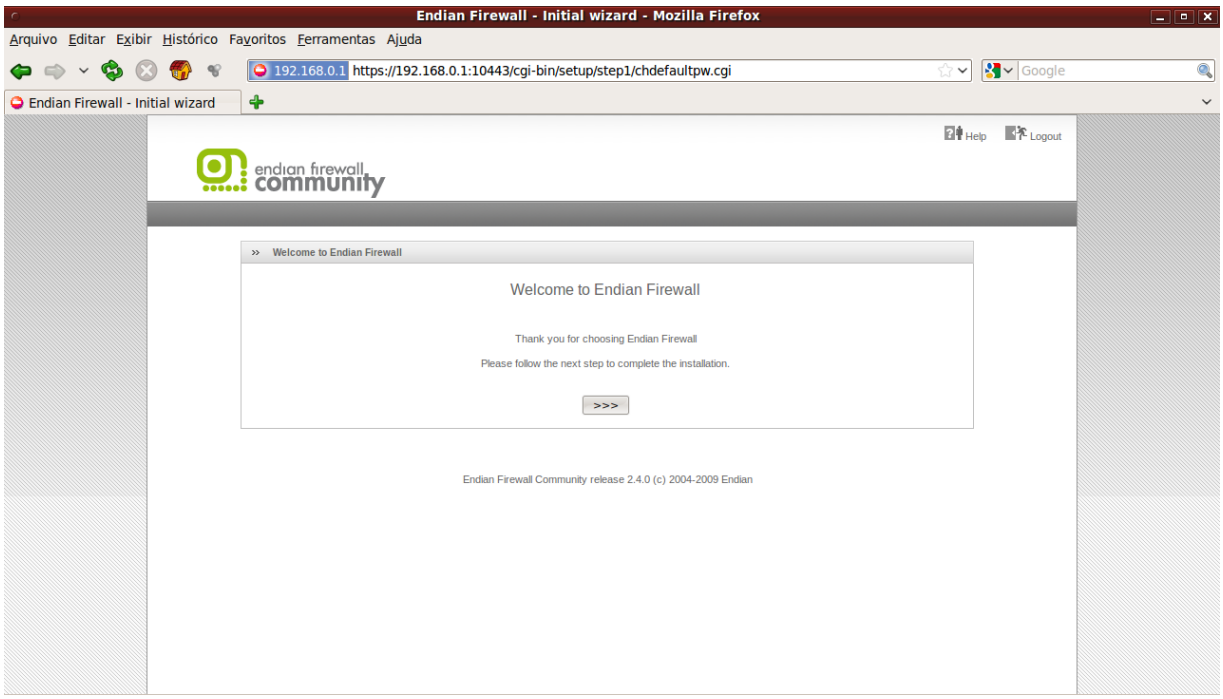


Ilustração 7: Página de boas vindas do Endian Firewall

Na página seguinte deverá ser selecionado o idioma “Português (Brasil)” para que toda a interface seja apresentado no nosso idioma. Após clique em “>>>”.

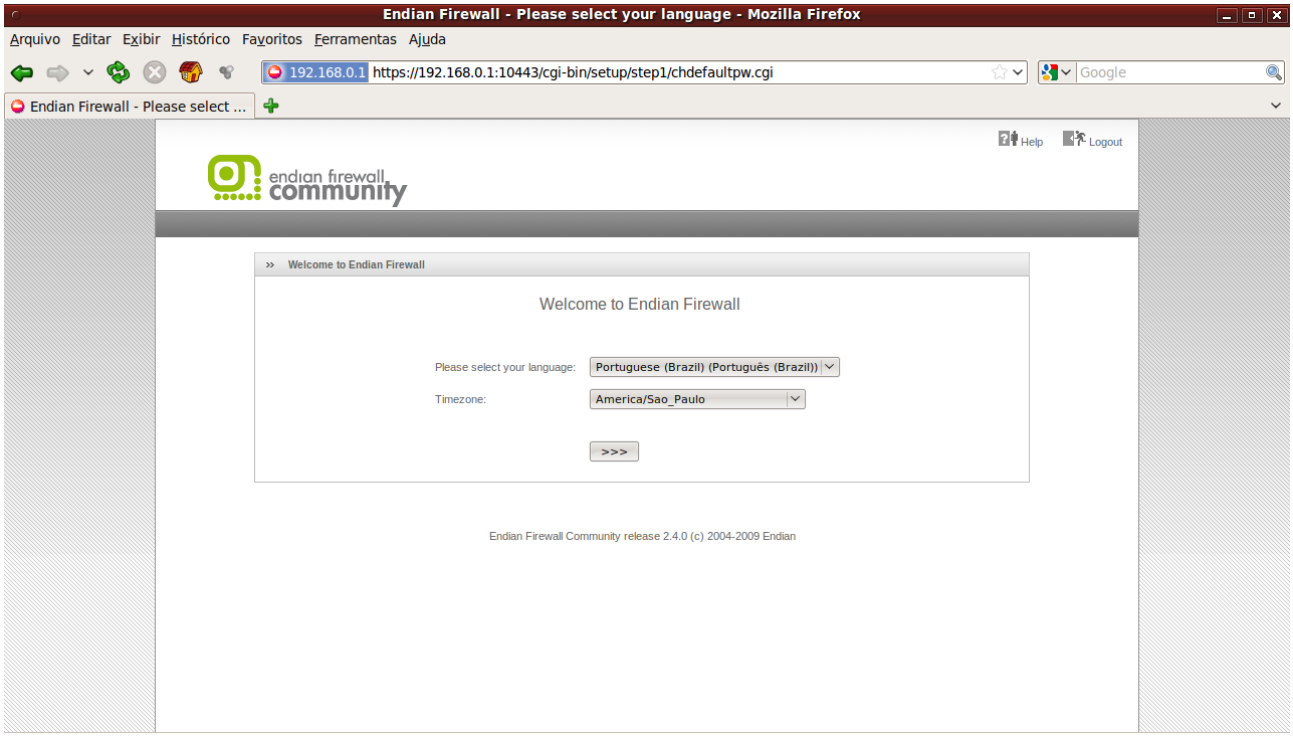


Ilustração 8: Página de seleção de idioma

A página seguinte apresenta a licença de uso livre (GPL) que deverá se aceita marcando a caixa “ACCEPT Licence” e clicando em “>>>”.

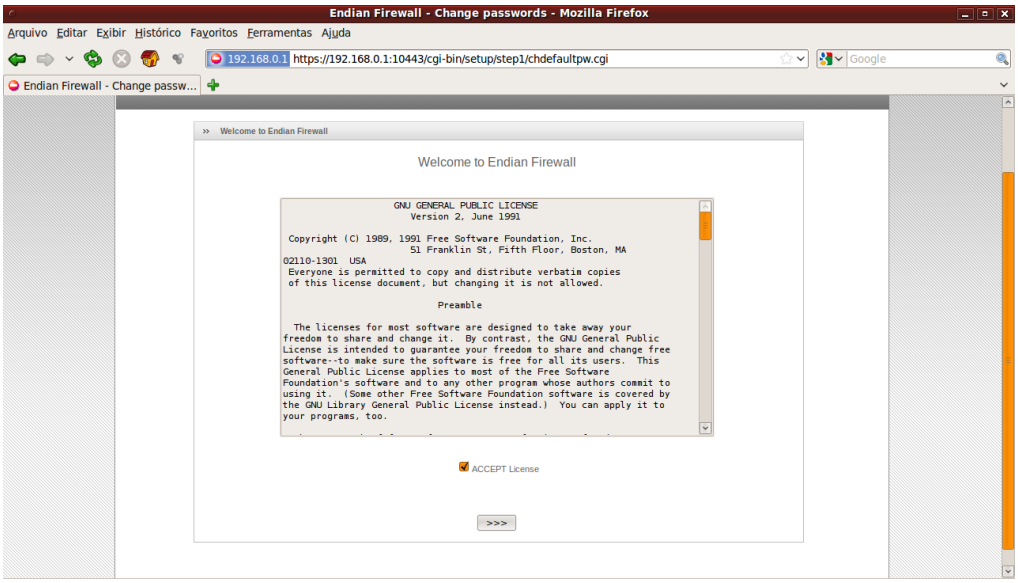


Ilustração 9: Apresentação da licença de uso

A próxima página é muito importante, caso você tenha pouco conhecimento sobre o assunto, recomendamos fortemente fazer a restauração do backup das configurações que encontram-se no diretório softwares do kit S.O.S. Esta configuração foi testada por nós, poupará tempo e foi adequada para operar no ponto Gesac com o menor uso possível dos recursos de rede.

Clique em “Sim” e restaure o arquivo **backup-conf-EndianFirewall-efw-gesac.localdomain-settings.tar.gz** que encontra-se no diretório **softwares**, o arquivo chama-se

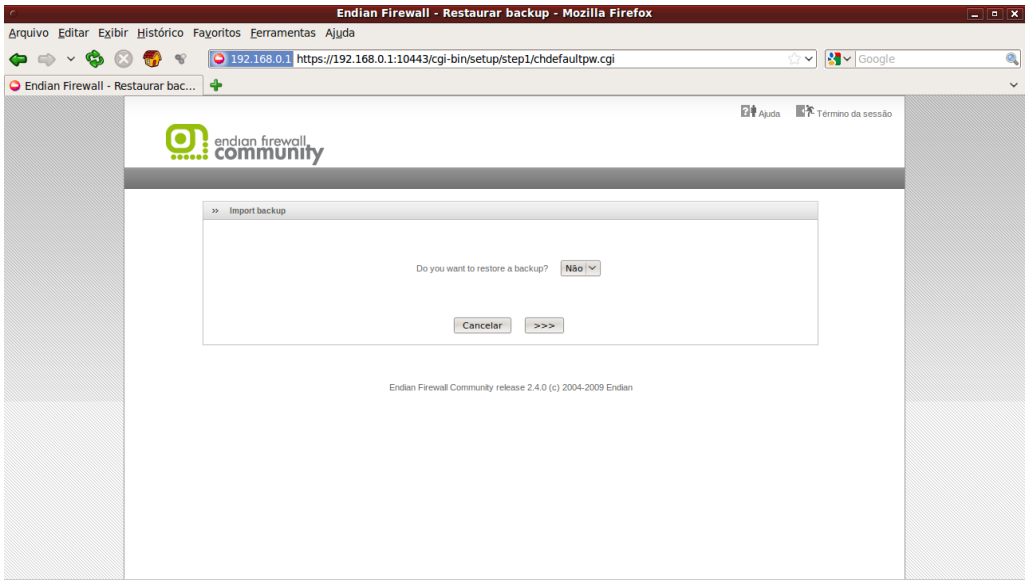


Ilustração 10: Restauração do backup

Caso tenha optado por fazer as configurações deverá ser definida a senha para acesso WEB e console no terminal local. Observo que 99,9% das necessidades de configuração serão resolvidas pela interface WEB. Desta forma, teremos os logins:

WEB – admin

Console - root

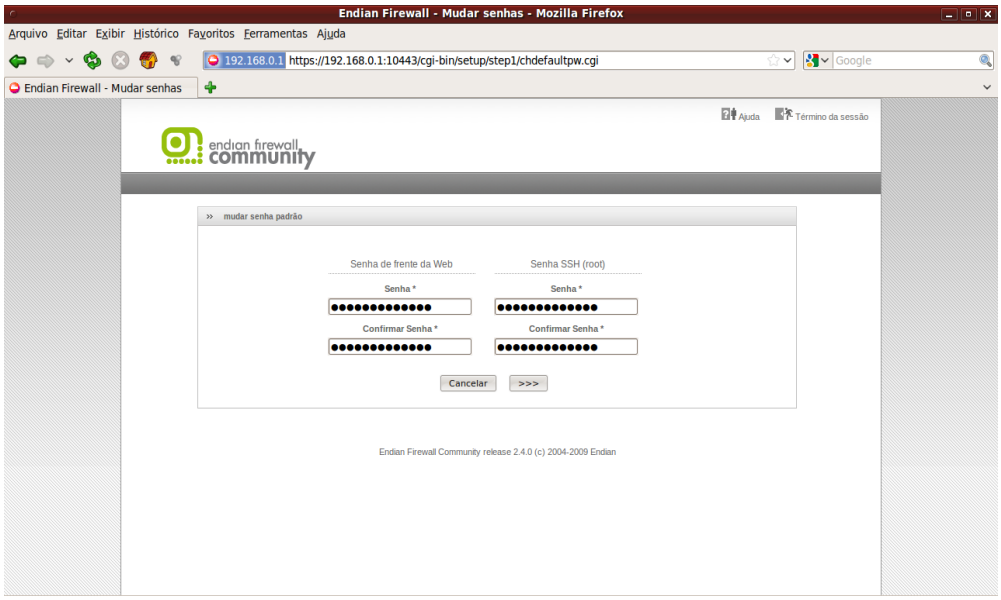


Ilustração 11: Definição da senha inicial para admin e root

A interface da rede Vermelha será ethernet DHCP. Clique em “>>>”.

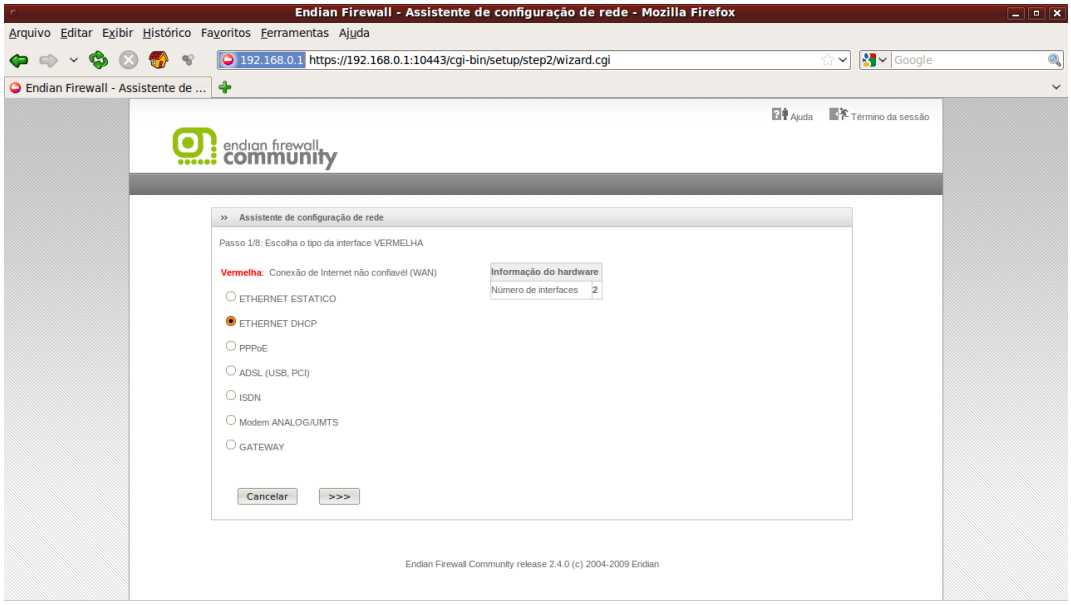


Ilustração 12: Definição do tipo de interface para rede Vermelha

Na janela seguinte é definida a interface e endereço IP para a rede interna. Geralmente nenhuma configuração é necessária. Clique em “>>>”.

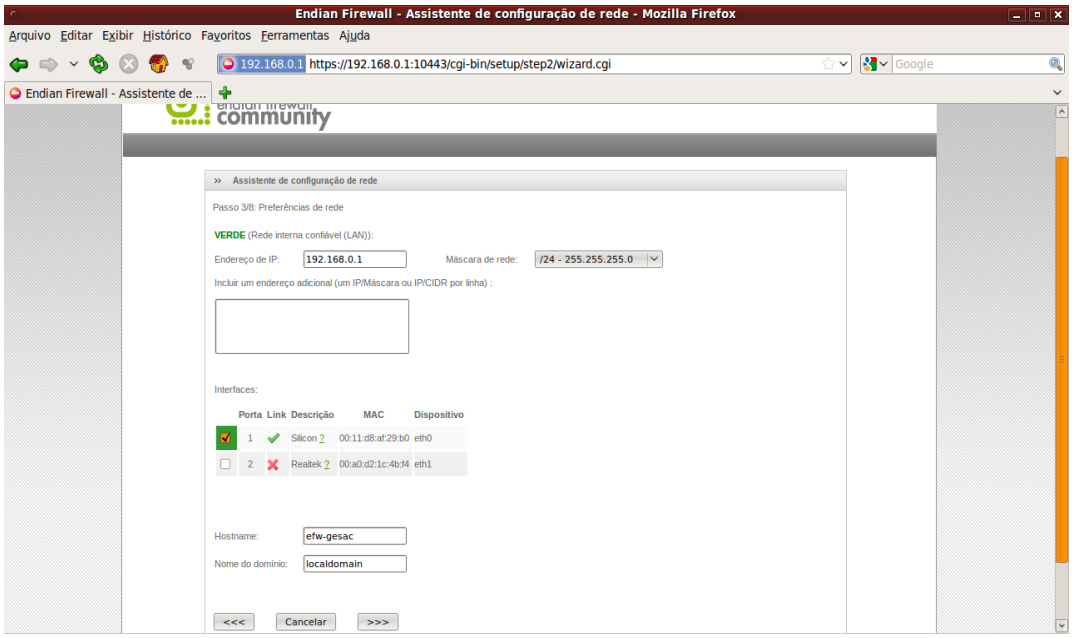


Ilustração 13: Configuração interface da rede Verde.

A próxima janela deverá ser marcada a interface livre para ser utilizada na rede Vermelha (X). Após clique em “>>>”.

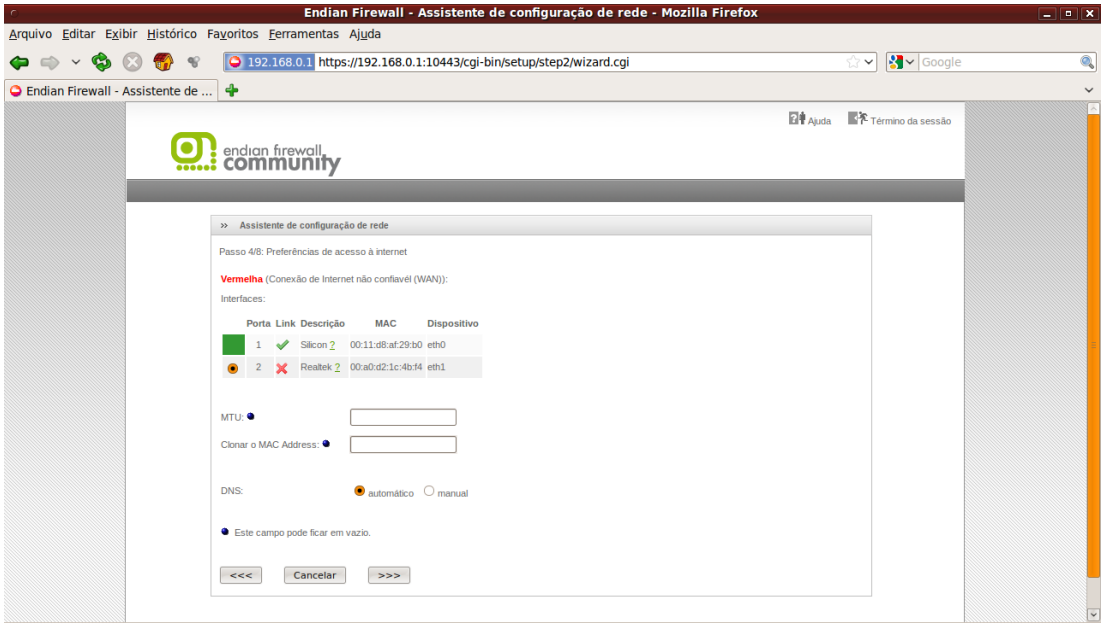


Ilustração 14: Definição da interface que será utilizada na rede Vermelha

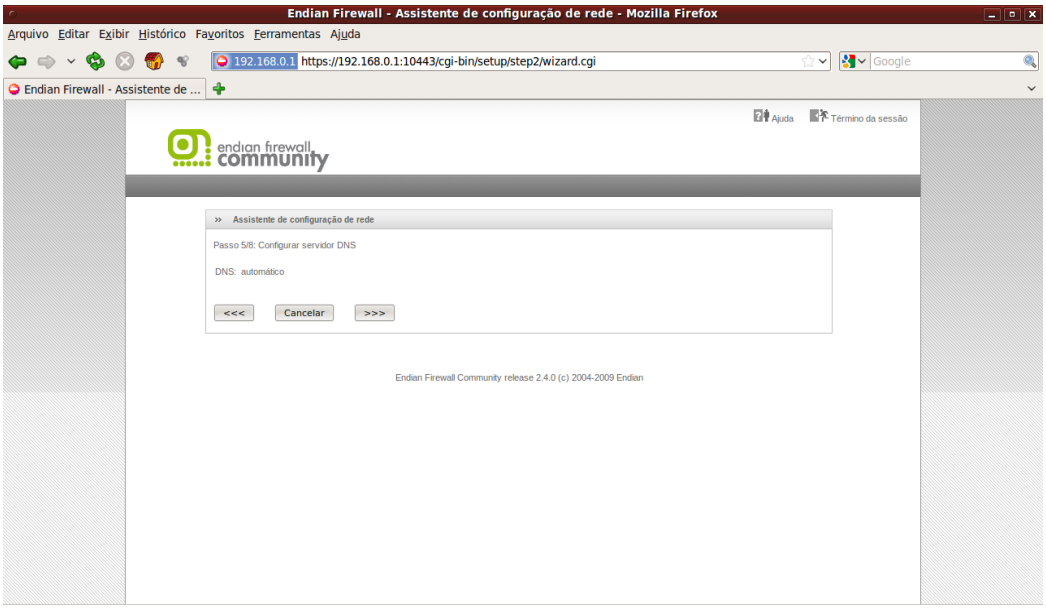


Ilustração 15: Servidor de DNS

Endian Firewall possui servidor de DNS interno para fazer proxy das consultas e acelerar o acesso a Internet. Clique em “>>>”.

Na próxima janela é possível definir email para receber as notificações do firewall por email. NÃO RECOMENDAMOS UTILZAR ESTA OPÇÃO, POIS CONSUMIRÁ BANDA DE INTERNET. Deixe em branco e clique em “>>>”.

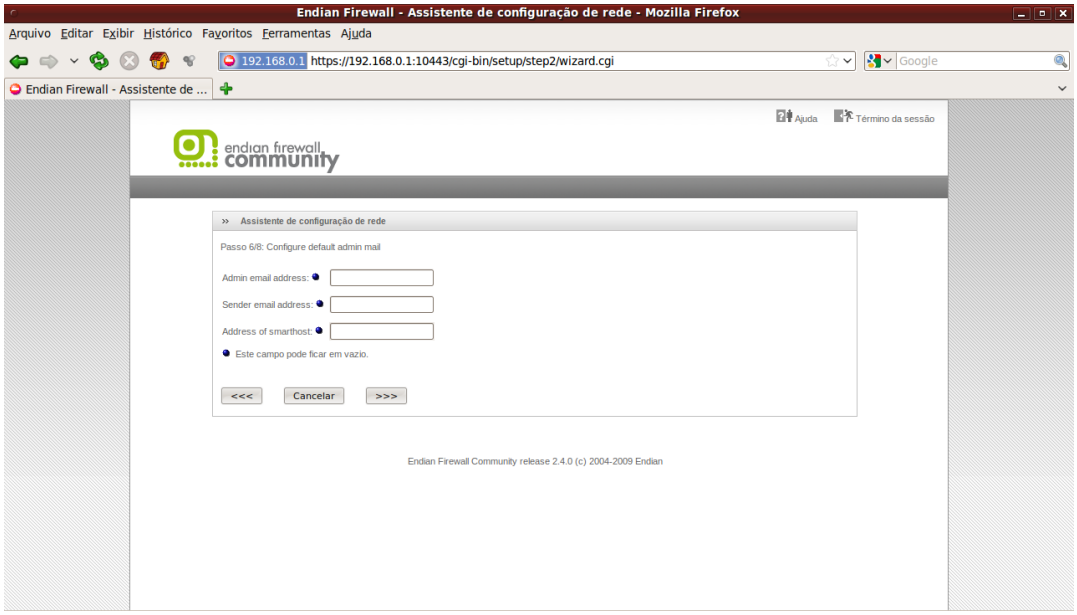


Ilustração 16: Notificações para email

Após clique em “Ok, aplicar configuração”.

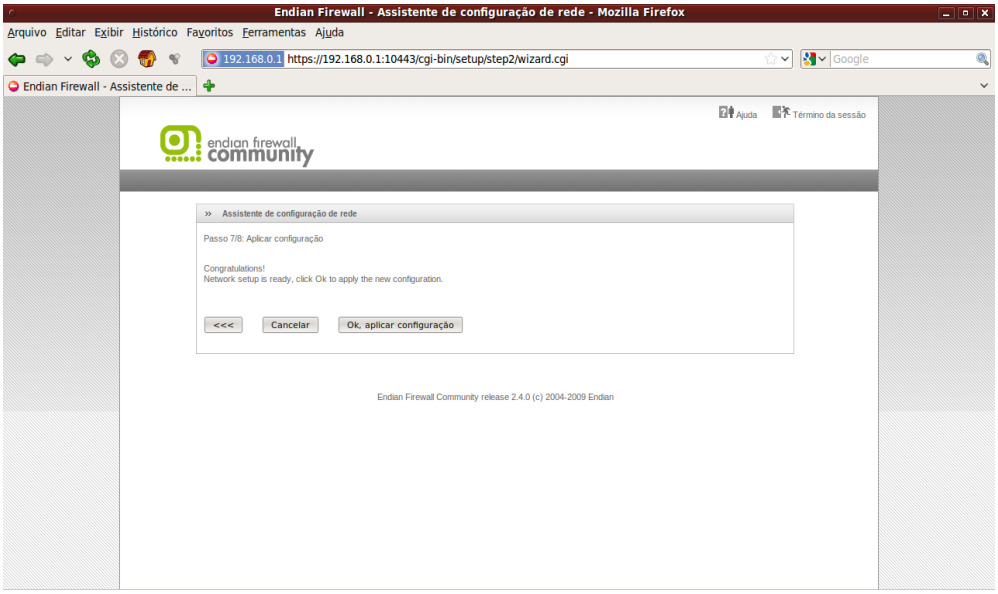


Ilustração 17: Janela final do primeiro acesso

4.4. Algumas janelas de configuração do Endian Firewall

O Endian Firewall possui uma interface WEB simples e muito prática que facilita a administração dos serviços de rede. Todos serviços são pré-instalados e configurados, cabendo apenas ativá-los e/ou algumas pequenas configurações.

4.4.1. Filtragem de pacotes

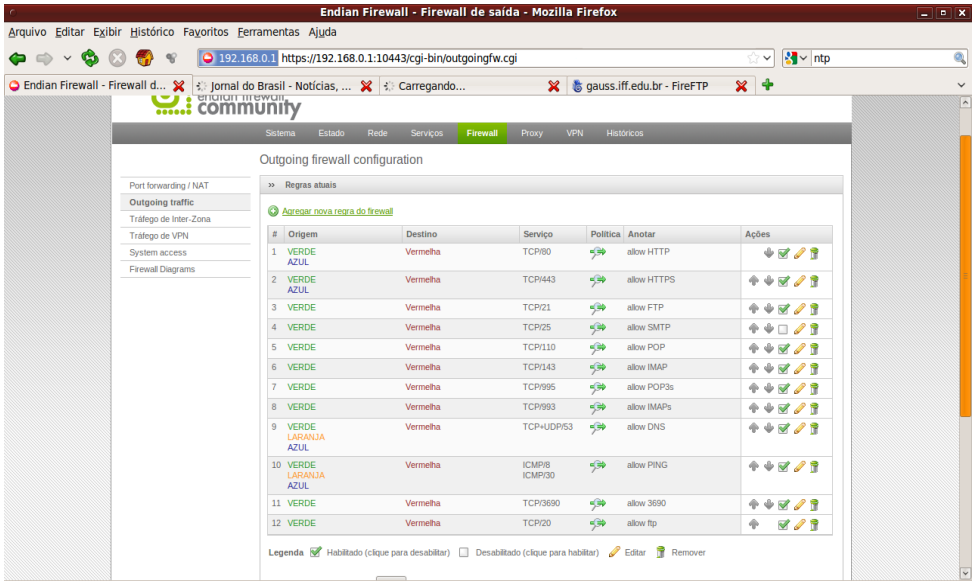


Ilustração 18: Interface para configurar o filtro de pacotes.

A configuração do filtro de pacotes é simples e muito prática. A seguinte páginas apresenta a configuração feita permitindo acesso da rede interna (verde) para a vermelha na porta 3690/TCP.

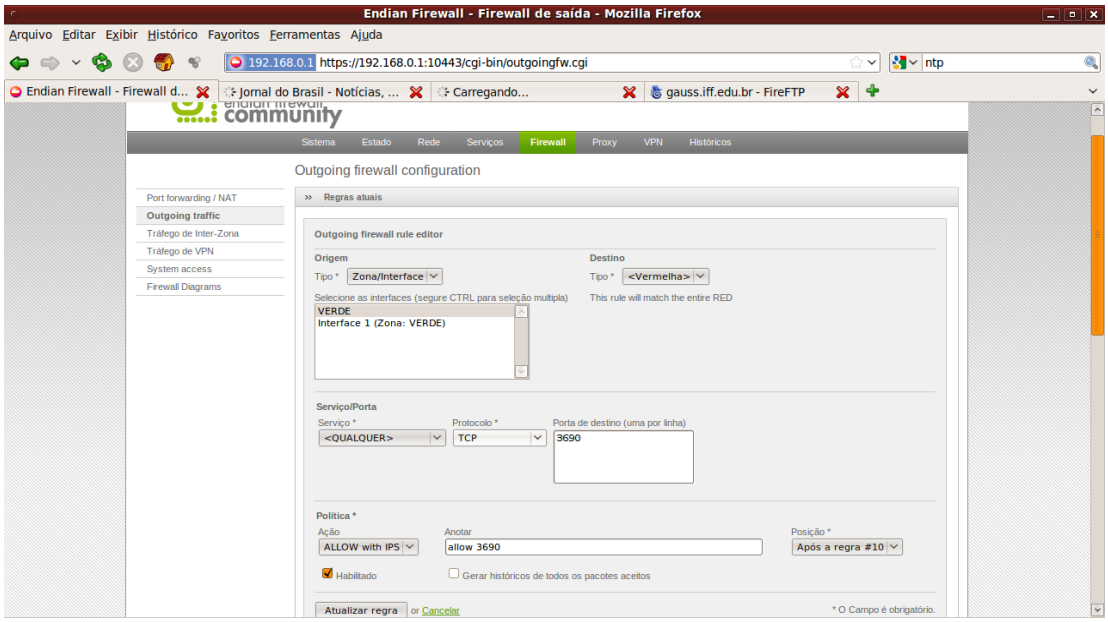


Ilustração 19: Exemplo da criação de uma nova regra

4.4.2. Proxy WEB

O serviço proxy WEB deve habilitado na forma transparente para melhorar o desempenho do acesso a Internet a partir da rede local do ponto GESAC.

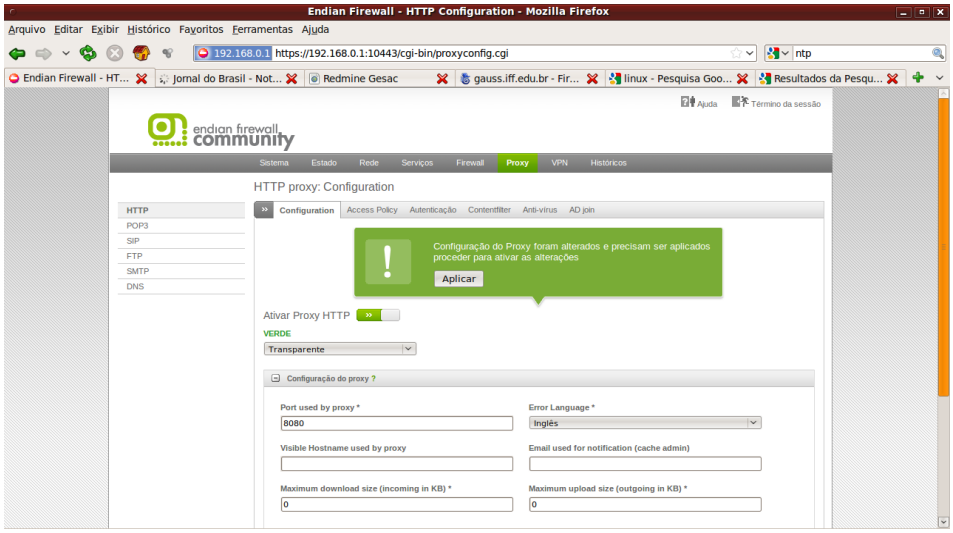


Ilustração 20: Configuração do Proxy WEB

Várias configurações podem ser realizadas para aumentar o desempenho. Uma delas é aumentar o tamanho do cache, memória RAM do proxy e tamanho máximo dos objetos no cache. Recomendamo utilizar pelo menos 1 GB para o tamanho do cache, reservar pelo menos 256 MB para memória ram do cache se firewall possuir 512 MB de ram e aumentar o tamanho máximo dos objetos no cache para valor entre 10 e 20 MB.

Também recomendamos habilitar o filtro de conteúdo Dansguardian e antivírus no acesso http e ftp. Estas configurações podem ser aplicadas restaurando o arquivo de backup que encontra-se no diretório softwares.

5. Bibliografia

COPYLEFT. In: Wikipédia, a enciclopédia livre. [S.l.], 2010. Disponível em: < http://pt.wikipedia.org/wiki/Copyleft >. Acesso em 04 out.2010.

DISTRIBUIÇÕES GNU/Linux Endian Firewall. <http://www.endian.com/ >. Acesso em 10 out. 2010.

PROTOCOLO IP. Disponível em 2010.: <http://pt.wikipedia.org/wiki/Protocolo_de_ Internet >. Acesso em 10 out.2010.

PROXY WEB. Disponível em: <http://pt.wikipedia.org/wiki/Proxy >. Acesso em 04 out.2010

STALLMAN, Richard. **The first software-sharing community**. In: The GNU Project. [S.l.]: Free Software Foundation, Inc., 2010. Disponível em: <http://www.gnu.org/gnu/the gnu project. Html >. Acesso em 04 out.2010

TCP. Rev. 15 out. 2010. Disponível em: < http://pt.wikipedia.org/wiki/TCP >. Acesso em 04 out. 2010.

WORRIOR on the net. Produção: Gunila Elam e Tomas Stephanson. Narração: Monte Reid. Música: Niklas Hanberger. [S.l.]: Media Lab, 2002. 1 vídeo (12 min), son., color. Disponível em: <http://www.warriorsofthe.net/>. Acesso em 15 out. 2010.

FORMAÇÃO

GESAC

CNPq Rede Federal GESAC Ministério da Educação Ministério das Comunicações