INSTITUTO FEDEREAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO ESPÍRITO SANTO CURSO SUPERIOR DE TECNOLOGIA EM REDES DE COMPUTADORES

EVERTON MOSCHEN BADA

Modelo de Configuração de Servidor para os Polos de Educação a Distância com o uso de Software Livre

SERRA
2010

EVERTON MOSCHEN BADA

Modelo de Configuração de Servidor para os Polos de Educação a Distância com o uso de Software Livre

Trabalho de Conclusão de Curso apresentado à Coordenadoria do Curso de Redes de Computadores do Instituto Federal de Educação, Ciência e Tecnológica do Espírito Santo, como requisito parcial para a obtenção do título de Tecnólogo em Redes de Computadores.

Orientador: Prof. José Inácio Serafini

SERRA

2010

EVERTON MOSCHEN BADA

Modelo de Configuração de Servidor para os Polos de Educação a Distância com o uso de Software Livre

Trabalho de Conclusão de Curso apresentado à Coordenadoria do Curso de Redes de Computadores do Instituto Federal de Educação, Ciência e Tecnológica do Espírito Santo, como requisito parcial para a obtenção do título de Tecnólogo em Redes de Computadores.

Aprovado em 26 de fev. de 2010

COMISSÃO EXAMINADORA

_____

Prof. José Inácio Serafini

Instituto Federal de Educação, Ciência e Tecnológica do Espírito Santo

Orientador

_____

Prof. M.Sc. Elton Siqueira Moura

_____

Prof. M.Sc. Sérgio Teixeira

DECLARAÇÃO DO AUTOR

Declaro, para fins de pesquisa acadêmica, didática e técnico-científica, que o presente Trabalho de Conclusão de Curso pode ser parcial ou totalmente utilizado desde que se faça referência à fonte e ao autor.

Serra, 26 de fev. de 2010

Everton Moschen Bada

Primeiramente agradeço a Deus.

A toda minha família que me apoiou em todos os momentos da minha vida.

Aos meus pais, que me deram a vida.

"O inteligente aprende com os seus erros.
Já o sábio aprende com os erros dos outros"

Apolo Doutrinador

“Nunca se considere no topo da montanha, pois

para qualquer lado que você andar só poderá descer,

então se considere no meio da montanha,

pois sempre terá um caminho para você subir.”

Autor desconhecido

RESUMO

Este trabalho apresenta uma proposta de um modelo de configuração de um servidor para os polos do Centro de Ensino A Distância do IFES. O modelo de servidor possuirá serviços como *firewall*, *Proxy*, DHCP e também proverá conexão de rede sem fio, e o mecanismo NAT, todos esses serviços sendo executados na distribuição Linux, conhecida como ZeroShell. No final do trabalho é apresentado um estudo de caso da configuração proposta.

Palavras-chave: ZeroShell, Firewall, Proxy, DHCP, NAT, Rede sem fio e CEAD.

ABSTRACT

This work presents a proposal for a model configuration of a server to the poles of the Education Distance Center. The server model will have services such as firewall, proxy, DHCP, and also provide connection to the wireless network, and NAT, all these services running on the Linux distribution, known as ZeroShell. At the end of the paper presents a case study of the proposed configuration.

Keywords: ZeroShell, firewall, proxy, DHCP, Wi-Fi, CEAD.

LISTA DE SIGLAS

CEAD- Centro de Educação A Distância

DHCP - *Dynamic Host Configuration Protocol*

EaD – Educação a Distância

GB - *Giga Byte*

GPL - *General Public License*

HAVP - *HTTP Antivírus Proxy*

HD – *Hard Disk*

HTTP- *Hypertext Transfer Protocol*

IFES – Instituto Federal de Educação Ciência e Tecnologia do Espírito Santo

IP – *Internet Protocol*

LAN – *Local Area Network*

NAT – *Network Address Translation*

RAM – *Random Access Memory*

TCP - *Transmission Control Protocol*

UAB - Universidade Aberta do Brasil

VPN – Virtual Private Network

Wi-Fi - *Wireless Fidelity*

LISTA DE FIGURAS

Figura 1: Tipos de *firewall* e sua atuação na camada OSI. 19

Figura 2: Estrutura do Proxy HAVP 22

Figura 3: Rede com servidor NAT 24

Figura 4: Rede CEAD com Wi-Fi 26

Figura 5: Página web de configuração do ZeroShell 28

Figura 6: Rede do CEAD do IFES 30

Figura 7: Rede do polo de apoio presencial 32

Figura 8: Página de *download* do ZeroShell. 37

Figura 9: resultado do comando fdisk -l 38

Figura 10: página de gerenciamento de *profiles* 40

Figura 11: página de gerenciamento de *profiles*, criando *profile* 41

Figura 12: Página de criação de novo *profile* 41

Figura 13: Página de configuração do DHCP 42

Figura 14: página de redirecionamento DNS 43

Figura 15: Página de configuração do NAT 44

Figura 16: Página de gerenciamento do Proxy 45

Figura 17: Página de configuração de *Black List* 46

Figura 18: Página de gerenciamento de interfaces de captura do Proxy 46

Figura 19: Página de criação de regras via comandos para o *firewall* iptables. 48

Figura 20: Página de gerenciamento do *firewall* 49

Figura 21: Página de criação de regra do *firewall iptables* via interface gráfica 50

Figura 22: Página de *backup* de *profile* 51

Figura 23: Página de restauração de *backup* 52

SUMÁRIO

1 INTRODUÇÃO 13

1.1 MOTIVAÇÃO 14

1.2 PROPOSTA DO TRABALHO 15

1.3 OBJETIVOS DO TRABALHO 16

1.4 METODOLOGIA 16

1.5 ESTRUTURA DA MONOGRAFIA 18

2 SERVIÇOS DE REDES E SEGURANÇA DA INFORMAÇÃO 19

2.1 FIREWALL 19

2.2 PROXY 21

2.3 DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) 22

2.4 NETWORK ADDRESS TRANSLATION (NAT) 23

2.5 WIRELESS FIDELITY (Wi-Fi) 24

2.6 ZEROSHELL 26

3 INFRAESTRUTURA DE REDE DO CEAD 29

3.1 O AMBIENTE DE UM POLO DE APOIO PRESENCIAL 30

3.2 REQUISITOS DO SERVIDOR 32

4 UMA PROPOSTA DE CONFIGURAÇÃO E SEUS BENEFICIOS 34

5 CONFIGURAÇÃO DE SERVIDOR E DOS SERVIÇOS 36

5.1 INSTALAÇÃO DO ZEROSHELL 36

5.2 CONFIGURAÇÃO DA INTERFACE DE REDE DO ZEROSHELL 38

5.3 CRIAÇÃO DE UM PROFILE 39

5.4 COFIGURAÇÃO DO DHCP 42

5.4.1 CONFIGURAÇÃO DO DNS 42

5.5 CONFIGURAÇÃO DO NAT 43

5.6 CONFIGURAÇÃO DO PROXY COM ANTIVÍRUS 44

5.7 CONFIGURAÇÃO DA REDE Wi-Fi 47

5.8 CONFIGURAÇÃO DO FIREWALL 48

5.9 BACKUP 50

5.9.1 REALIZAR *BACKUP* 50

5.9.2 RESTAURAR O *BACKUP* 52

6 CONSIDERAÇÕES FINAIS E RESULTADOS 53

6.1 TRABALHOS FUTUROS 54

7 REFERÊNCIAS BIBLIOGRÁFICAS 55

1 INTRODUÇÃO

De acordo com uma pesquisa do site *INTERNET WORLD STATES* (*INTERNET WORLD STATES,* 2010) a Internet na America Latina cresceu 890,0%, no ano de 2009 na América Latina 30 % da população possuía acesso a Internet. A difusão do acesso a Internet na América Latina e, conseqüentemente, no Brasil, viabilizou a Educação a Distância (EaD) por meio da Internet, como uma alternativa ao ensino presencial.

Com o investimento do governo em educação a distância desde 2005, através do sistema Universidade Aberta do Brasil, a EaD ganhou força e está presente em várias instituições espalhadas pelo Brasil. Segundo o site oficial da UAB (UAB, 2010c), 88 instituições integram o sistema, entre universidades federais, universidades estaduais e Institutos Federais de Educação, Ciência e Tecnologia (IFES). Segundo a UAB (UAB, 2010c) de 2007 a julho de 2009 foram aprovados 557 polos com 187.154 vagas.

O Centro de Educação a Distância (CEAD) do Instituto Federal do Espírito Santo (IFES) começou a oferecer cursos a distância desde 2006, em parceria com as prefeituras dos municípios do estado do Espírito Santo, através do sistema UAB. Os polos localizados nos municípios são pertencentes às prefeituras das respectivas cidades e o CEAD se localiza no IFES campus Serra.

Os polos se comunicam com o CEAD através da Internet, cada polo possui acesso banda larga à Internet para viabilizar essa comunicação. A infraestrutura de rede é de grande importância na EaD, pois é através dela que os alunos tem acesso aos materiais e aos tutores. Com isso conclui-se que é de extrema importância que a rede dos polos esteja funcionando o maior período de tempo possível, para evitar transtornos aos alunos e para aumentar a qualidade do ensino.

Para auxiliar na tarefa de manter a rede dos polos funcionando a maior parte do tempo possível existem várias tecnologias, softwares e protocolos. É possível padronizar a configuração dos servidores facilitando assim a instalação, configuração, a manutenção e o suporte.

Um servidor com os serviços de Firewall, Proxy, DHCP, entre outros serviços auxilia na segurança, na gerência e na manutenção da rede dos laboratórios dos polos de EaD.

1.1 MOTIVAÇÃO

A UAB especifica todos os requisitos de equipamentos, instalações e pessoal para os polos de EaD, sem atender a esses requisitos um polo não pode ser criado. Entretanto esta especificação não abrange o nível lógico da rede, somente abrange a parte física de equipamentos. Com isso, cada polo pode criar sua própria estrutura lógica, com servidores ou não, equipamentos de segurança ou não. Isto gera uma heterogeneidade dificultando o suporte aos polos e, conseqüentemente, gerando transtornos aos alunos.

No projeto lógico de configuração dos polos de EaD não existe um modelo de configuração dos servidores dos polos. Essa falta de padronização ocasiona alguns transtornos para a gestão dos polos. Quando ocorre algum problema específico de configuração de servidor (quando existe) ou na rede de algum polo, muitas vezes o problema persiste-se muito tempo pois nem sempre os pólos possuem um profissional qualificado em redes e segurança para solucionar determinados problemas. Com a padronização dos servidores dos pólos e com um servidor de fácil configuração e manutenção, essa questão seria amenizada.

A especificação de um modelo de configuração de servidor para os polos pode permitir a padronização de configuração e uso da rede, facilitando a manutenção e suporte na ocorrência de eventuais problemas.

O acesso de usuários remotos por meio de rede sem fio, as políticas de segurança

e a configuração de aplicativos específicos para os cursos a distância do CEAD poderá ser padronizado e configurado remotamente pelo CEAD, pois a interface web do aplicativo de configuração do servidor proposto permite o suporte remoto com pouca intervenção de profissionais locais dos polos.

1.2 PROPOSTA DO TRABALHO

Este trabalho aborda o problema da falta de um servidor, com serviços que possam prover o mínimo de segurança para os laboratórios dos polos de apoio presencial. A falta de um modelo de configuração de um servidor que faz o papel de Firewall, Proxy, dentre outros serviços necessários para o funcionamento da rede do pólo, deixará os recursos computacionais vulneráveis ao ataque ou acesso indevido de intrusos na rede.

No modelo de funcionamento dos pólos a administração é feita pela prefeitura da cidade, pois existe uma parceria firmada que estabelece um convênio. No modelo de convênio já existe uma definição de como deve ser o polo, entretanto, não existe a especificação de um servidor ou roteador, incluindo sua configuração para ser usado no polo. Diante disso, cada polo faz a configuração de uma forma diferente, gerando uma falta de padronização no suporte para o funcionamento do acesso à Internet.

Para ajudar solucionar esse problema é proposto um modelo de configuração de um servidor de polo para padronizar a forma de funcionamento em todos os polos e facilitar a manutenção e suporte em caso de problemas. Foi proposta a utilização do sistema ZeroShell no servidor dos polos que integra e utiliza os seguintes serviços em um único equipamento:

- *Firewall*;
- *Proxy* com antivírus integrado;

- *DHCP;*

- Balanceamento de carga.

Os serviços do ZeroShell podem ser configurados por meio de interface web, facilitando a manutenção e suporte remoto em caso de problemas.

1.3 OBJETIVOS DO TRABALHO

O objetivo geral deste trabalho é propor um modelo de configuração de um servidor, incluindo as especificações mínimas de hardware, softwares e o sistema operacional para ser utilizado nos polos de EaD. O modelo de configuração proposto utilizará softwares livres, proporcionando segurança, eficácia e facilidade de reinstalação em caso de problemas. Além disso, o trabalho tem os seguintes objetivos específicos:

- Propor um modelo de configuração do servidor, utilizando Firewall, Proxy, Antivírus, DHCP e *Access Point* e roteador de rede sem Wi-Fi;

- Disponibilizar uma rede Wi-Fi com criptografia WAP2;

- Definir uma política de segurança de acesso à Internet;

- Especificar o funcionamento do antivírus;

1.4 METODOLOGIA

Na aula de Trabalho de Conclusão de Curso foi organizada, por meio do professor Gilmar Luis Vassoler, uma palestra com todos os professores com intenção de orientar alunos, esses professores, por sua vez, apresentaram suas propostas. O professor José Inácio Serafini apresentou uma proposta de trabalho muito interessante, criar um modelo de configuração de servidor para os polos. Essa necessidade foi percebida por ele através de seus trabalhos realizados no CEAD.

Com isso, resolvemos estudar mais afundo este assunto e este problema, para propormos uma solução. Começou-se a estudar o CEAD, com sua estrutura e como ele trabalha, quais são suas ligações com os polos e quais cursos eram oferecidos e de que forma isso ocorria. Com estes estudos percebeu-se a necessidade de um servidor padronizado, com tecnologias, protocolos e serviços específicos para os polos. Em conseqüência disso foi feito um esboço inicial das necessidades para o servidor dos polos.

Após a caracterização mais específica da necessidade de um servidor e sua configuração em um polo foi feita uma revisão bibliográfica das tecnologias e sistemas disponíveis para à proposta de trabalho. Além disso, foi feita uma revisão bibliográfica de trabalhos correlatos e não foi identificado nenhum trabalho similar à proposta de configuração de um servidor para polo.

Após a revisão bibliográfica foi identificado que existe uma distribuição Linux voltada especificamente para fazer o papel de servidor de firewall, Proxy, DHCP, NAT entre outros serviços, denominado ZeroShell. O ZeroShell é uma distribuição do sistema operacional Linux e ao mesmo tempo um servidor do serviços próprios para apoiar pequenas redes de computadores, provendo segurança e acesso sem fio.

Com objetivo de conhecer melhor o ZeroShell e verificar que realmente pode ser aplicado ao uso nos polos foi feita a instalação de um protótipo para usar e testar os recursos oferecidos.

Após constatar que o ZeroShell atende ao objetivo proposto foi feita uma revisão bibliográfica de todos os serviços, tecnologia e protocolos utilizados pelo ZeroShell.

Com o conhecimento mais detalhado das funcionalidades e possibilidades do ZeroShell foi feito um estudo de caso com a instalação de um servidor para simular o funcionamento de um polo. Com isso, foi possível testar e verificar que

tudo que foi idealizado e proposto poderia ser feito com o ZeroShell.

Por fim, foi feito o registro do passo a passo de instalação e configuração do servidor, identificando as configurações do hardware e do software com objetivo de auxiliar futuramente profissionais do CEAD que queiram instalar o modelo de configuração proposto em algum polo.

1.5 ESTRUTURA DA MONOGRAFIA

Este capítulo trata da introdução e da apresentação da proposta deste trabalho. O capítulo 2 apresenta tecnologias, serviços e protocolos que são utilizados no modelo de configuração proposto com o uso do sistema ZeroShell. O capítulo 3 apresenta a infraestrutura de rede do CEAD e de seus polos. O capítulo 4 apresenta o modelo de configuração de servidor proposto com o uso do ZeroShell. O capítulo 5 apresenta um estudo de caso de um servidor de polo que foi configurado com o modelo proposto para testar os serviços do ZeroShell. O capítulo 6 apresenta a conclusão deste trabalho e, por fim, o capítulo 7 apresenta as referências bibliográficas utilizadas nesse trabalho.

2 SERVIÇOS DE REDES E SEGURANÇA DA INFORMAÇÃO

Neste capitulo, será apresentada uma descrição dos principais serviços, tecnologias e protocolos utilizados no trabalho. A compreensão do ZeroShell depende do entendimento desses serviços, pois o ZeroShell implementa esses conceitos.

2.1 FIREWALL

O *firewall* é um dispositivo de segurança que filtra o trafego de dados da rede, normalmente se localiza entre a rede que se deseja proteger e a rede da qual precisa ser protegida. O *firewall* é configurado com um conjunto de regras, que analisam os campos do cabeçalho dos pacotes para decidir se determinado tráfego de dados vai ser bloqueado ou não. Esse conjunto de regras pode ser baseado em várias informações que podem estar presentes no fluxo de dados, por exemplo, um *firewall* pode filtrar um fluxo de dados pela porta de destino, pelo protocolo do pacote, entre outros (KUROSE, 2006).

A figura 1 apresenta os tipos de *firewall* e sua atuação no modelo de referência OSI. Esta figura é uma adaptação de (MELO, 2006).

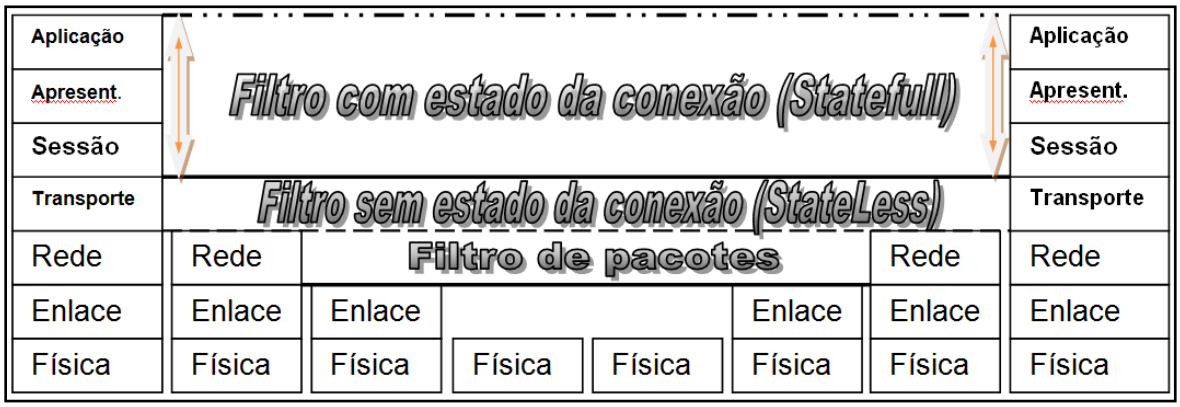


Figura 1: Tipos de *firewall* e sua atuação na camada OSI.

Fonte: (MELO, 2006).

O *firewall* pode ser classificado de acordo com seu nível de atuação na pilha de protocolos, como é mostrado na figura 1. Caso o *firewall* consiga atuar somente na camada de rede, este é classificado como filtro de pacotes (*Packet Filter*), caso atue até a camada de transporte, é classificado como filtro de pacotes sem estado de conexão (*StateLess Packet*), e se atuar em todas as camadas da pilha de protocolo ele é chamado de filtro com estado da conexão (*StateFull Packet*).

Um *firewall* do tipo filtro de pacotes somente pode filtrar um tráfego de dados baseado nos protocolos e informações que estão disponíveis até a camada de rede, como endereço MAC de origem/destino, endereço IP de origem/destino, protocolos do tipo ICMP ou IP, interface de E/S (I/O) ou tamanho do pacote (MELO, 2006).

Caso um *firewall* seja do tipo filtro de pacotes sem estado da conexão, ele pode trabalhar com todas as informações que um *firewall* do tipo filtro de pacotes atua, com adição das informações, porta de origem/destino, protocolos TCP ou UDP, número de conexões paralelas e número do fragmento (STREBE e PERKINS, 2002).

Caso um *firewall* seja do tipo filtro com estado de conexão, ele pode atuar com informações de toda pilha de protocolos, como estado da conexão, protocolos da camada de aplicação, entre outros (MELO, 2006).

O *firewall* que será utilizado por este projeto é o *iptables* (KUROSE, 2006), por atuar em toda a pilha TCP/IP, ou seja, ser *StateFull*, e por ser um dos mais difundidos atualmente. O *iptables* trabalha com três cadeias de filtros, são elas: *INPUT* (entrada), *OUTPUT* (saída) e a *FORWARD* (encaminhamento). Todo o fluxo de dados, que passa pelo *firewall*, será tratado por pelo menos uma dessas cadeias, que contém regras que liberam ou negam a passagem de um fluxo de dados (NAKAMURA, 2007).

Caso um pacote seja destinado à máquina *firewall* este pacote será tratado pela cadeia *INPUT,* então todas as regras de filtragem que se deseja para esses tipos de pacotes devem estar localizadas nessa cadeia (STREBE, 2002).

Caso um pacote seja originado na máquina firewall para ser transmitido, esse

pacote será tratado pela cadeia *OUTPUT,* então todas as redes de filtragem que se deseja para esses tipos de pacotes devem estar localizadas nessa cadeia. (STREBE, 2002).

Caso um pacote seja roteado pela máquina firewall, ou seja, passe por ela e vai para outra rede/máquina, este será tratado pela cadeia *FORWARD*, então todas as regras para esse tipo de pacote devem estar localizadas nesta cadeia.

Para que o *iptables* filtre o que é necessário, as regras presentes em suas cadeias de filtros devem estar bem definidas e configuradas de acordo com as necessidades de segurança da rede.

O *firewall* é uma importante ferramenta de segurança, mas trabalhando em conjunto com o Proxy fornece maior nível de segurança (MOURANI, 2001).

2.2 PROXY

Segundo Lima (LIMA, 2003) o *proxy* surgiu da necessidade de conectar uma rede local a Internet através de um computador da rede que compartilha sua conexão com as demais máquinas, ou seja, o *proxy* faz o papel de intermediador da comunicação.

O *proxy* atua entre a rede, que deseja ser protegida e a rede da qual se deseja proteger, normalmente se localiza na mesma máquina que o *firewall*, pois, podem trabalhar em conjunto. O *proxy* além de fazer a intermediação da comunicação também faz o controle de acesso dos usuários, isso é feito de forma bem simples e flexível através de listas de controle de acesso (*Access Control List* – ACL), onde se localizam as regras de filtragem. Esses filtros determinam qual conteúdo das páginas que podem ser acessados, entre outras funcionalidades.

O Proxy HAVP *(HTTP Antivirus Proxy)* foi criado por Christian Hilgers e fornece as funcionalidades de *Black List*, *White List,* e ainda a funcionalidade de antivírus, que verifica as imagens JPG, PNG e GIF contra vírus e, conseqüentemente, gera

LOG de todas as páginas que contém vírus (RICCIARD, 2009), (HILGERS, 2010).

O Proxy foi uma criação do próprio Hilgers, já o antivírus ele utilizou o ClamAv, que é livre. O proxy HAVP possui a estrutura ilustrada na figura 2, onde o fluxo originado pelo cliente passa pelo Proxy, então é verificado o *white* e o *Black List*, caso esteja liberado, o trafego passa, caso contrário retorna a página de bloqueio. Já o fluxo originado na Internet, passa pelo Proxy, e é armazenado em forma de arquivo temporário e o antivírus ClamAv, analisa o arquivo, caso tudo esteja certo, o trafego é enviado ao cliente.

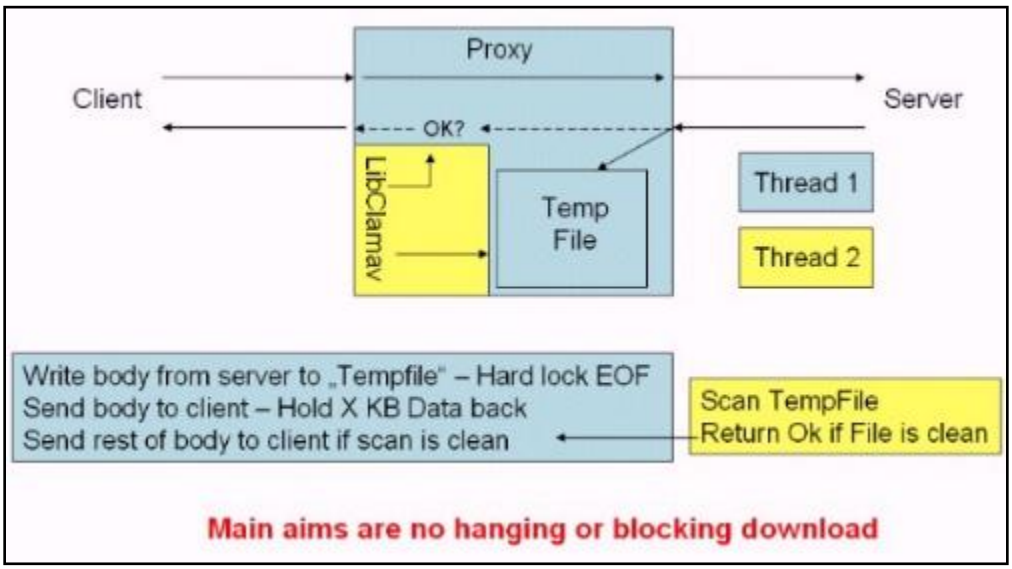


Figura 2: Estrutura do Proxy HAVP

Fonte: (HILGERS, 2010)

2.3 DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)

Segundo Lima (LIMA, 2003) DHCP é um acrônimo para protocolo de configuração dinâmica de computador (*Dinamic Host Configuration Protocol*). Lima (LIMA, 2003) diz que o DHCP é um protocolo cliente/servidor, que possibilita computadores clientes receberem configuração TCP/IP dinamicamente.

Após ligar um cliente DHCP é feita a solicitação de configuração de rede ao servidor de DHCP existente na rede. Em seguida, o servidor fará o envio das configurações de rede de acordo com as configurações do servidor de DHCP.

Após o recebimento das configurações o cliente DHCP confirma o recebimento. O servidor registra a informação que será guardada até a data de expiração da configuração fornecida.

O software *dhcp server* é um bom servidor DHCP, possuindo todas as funcionalidades de um servidor dhcp necessário para redes locais.

2.4 *NETWORK ADDRESS TRANSLATION* (NAT)

Segundo Donaldson (DONALDSON, 2009) NAT é um mecanismo que permite a tradução de um endereço do protocolo da Internet (endereço IP) utilizado dentro de uma rede para um diferente endereço IP conhecido em outra rede. Segundo Battisti (BATTISTI, 2009) o NAT surgiu como uma alternativa real para a falta de endereços IPv4 na Internet.

O uso de NAT possibilita que as máquinas da rede interna utilizem endereços IP reservados conhecidos como endereços privados, ou seja, só funcionam dentro de uma rede interna. Eles não são válidos para trafegarem na Internet, pois quando essas máquinas se comunicam com a Internet o mecanismo NAT faz a tradução do IP privado para um IP público válido.

As faixas de IP que são reservadas são as seguintes:

- 127.0.0.0 -> 127.255.255.255
- 10.0.0.0 -> 10.255.255.255
- 172.16.0.0 -> 172.31.255.255
- 192.168.0.0 -> 192.168.255.255

Como um endereço IP privado não é válido para trafegar na Internet, a máquina que executa o NAT, traduz o endereço IP privado para um endereço IP público válido. Para melhor exemplificar veja a figura 3, considere que a máquina com

endereço IP 192.168.1.2 deseje enviar um pacote para uma máquina na Internet com endereço de 200.221.40.15. Quando o pacote chegar ao servidor NAT o endereço de origem será substituído por 200.10.50.30.18, que é um endereço válido na Internet, quando a máquina de IP 200.221.40.15 for responder a esse pacote, o endereço de destino será o 200.10.50.30.18, então esse pacote chegará ao servidor NAT, e esse por sua vez o re-encaminhará à máquina com o IP 192.168.1.2.

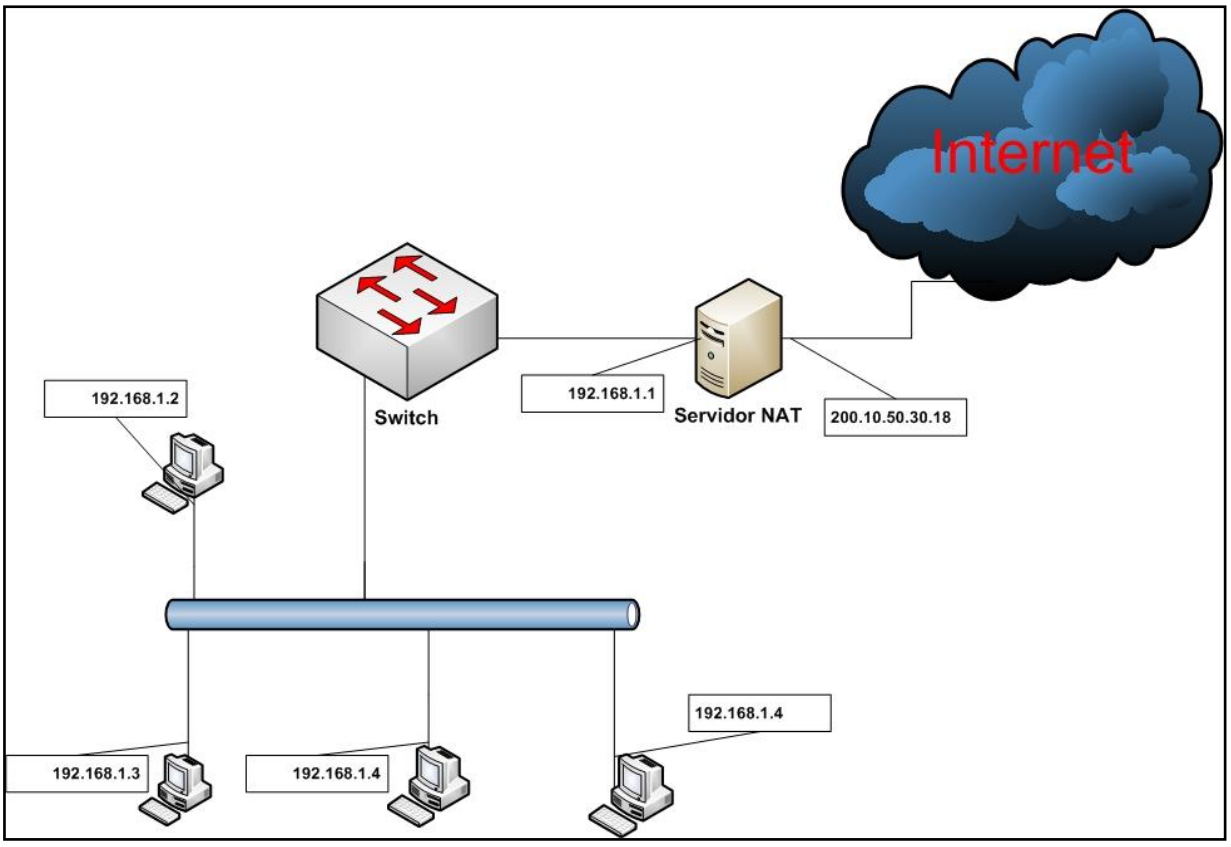


Figura 3: Rede com servidor NAT

O iptables mesmo software que faz a função de *firewall*, também faz a função de NAT. O iptables é um dos softwares livres mais utilizados para a função de firewall e NAT.

2.5 WIRELESS FIDELITY (Wi-Fi)

Segundo Alecrim (ALECRIM, 2009) Wi-Fi é um conjunto de especificações para

redes locais sem fio. O Wi-Fi é baseado no padrão IEEE 802.11, que define redes locais sem fio. A entidade Wi-Fi *alliance* (WiFi *Alliance*, 2009), que é a principal responsável pelo licenciamento de produtos desse padrão, afirma que uma rede Wi-Fi utiliza a tecnologia de rádio chamada de 802.11 para prover uma conexão de rede sem fio rápida, segura e confiável.

As redes sem-fio, como qualquer outra rede, necessita prover segurança. Nas redes sem fio um dos modos de segurança é a criptografia dos dados. Para prover a criptografia existem vários modos, entre os mais conhecidos estão a *wired equivalent privacy* (WEP, em português Privacidade Equivalente a Rede Cabeada) e a *Wi-Fi Protected Access* (WPA, em português Acesso Wi-Fi Protegido).

De acordo com o site vivasemfio.com (VIVASEMFIO, 2010) o WEP foi criado por alguns membros do IEEE, para proteger o fluxo de dados entre os equipamentos Wi-Fi. De acordo com Bradley (BRADLEY, 2010) WEP é o esquema de encriptação de dados presentes nos primeiros equipamentos de rede *wireless.* Mas foram encontradas algumas falhas graves, que tornam relativamente fácil, a quebra da encriptação, por isso não é a melhor forma de se proteger uma rede wireless.

Devido às vulnerabilidades do WEP a *Wi-Fi Alliance* adiantou a parte de autenticação e cifração do padrão 802.1i, ele utiliza o protocolo *Temporal Key Integrity Protocol* (TKIP), uma tecnologia de encriptação mais avançada do que o RC4 da WEP.

Os softwares que serão utilizados para prover conexão Wi-Fi serão os seguintes:

- *Wireless Tools*- Gerenciamento de interfaces *wireless*;
- *MadWIFI* - Módulo do kernel para placas de rede Wi-Fi;
- *WPA-Supplicant* - Autenticação WPA/WPA2 para clientes;
- *HostAP daemon* - Autenticação WPA/WPA2 para *access point*;

Segundo Fulvio (RICCIARD, 2009) estas são as ferramentas padrão para essas funcionalidades do ZeroShell.

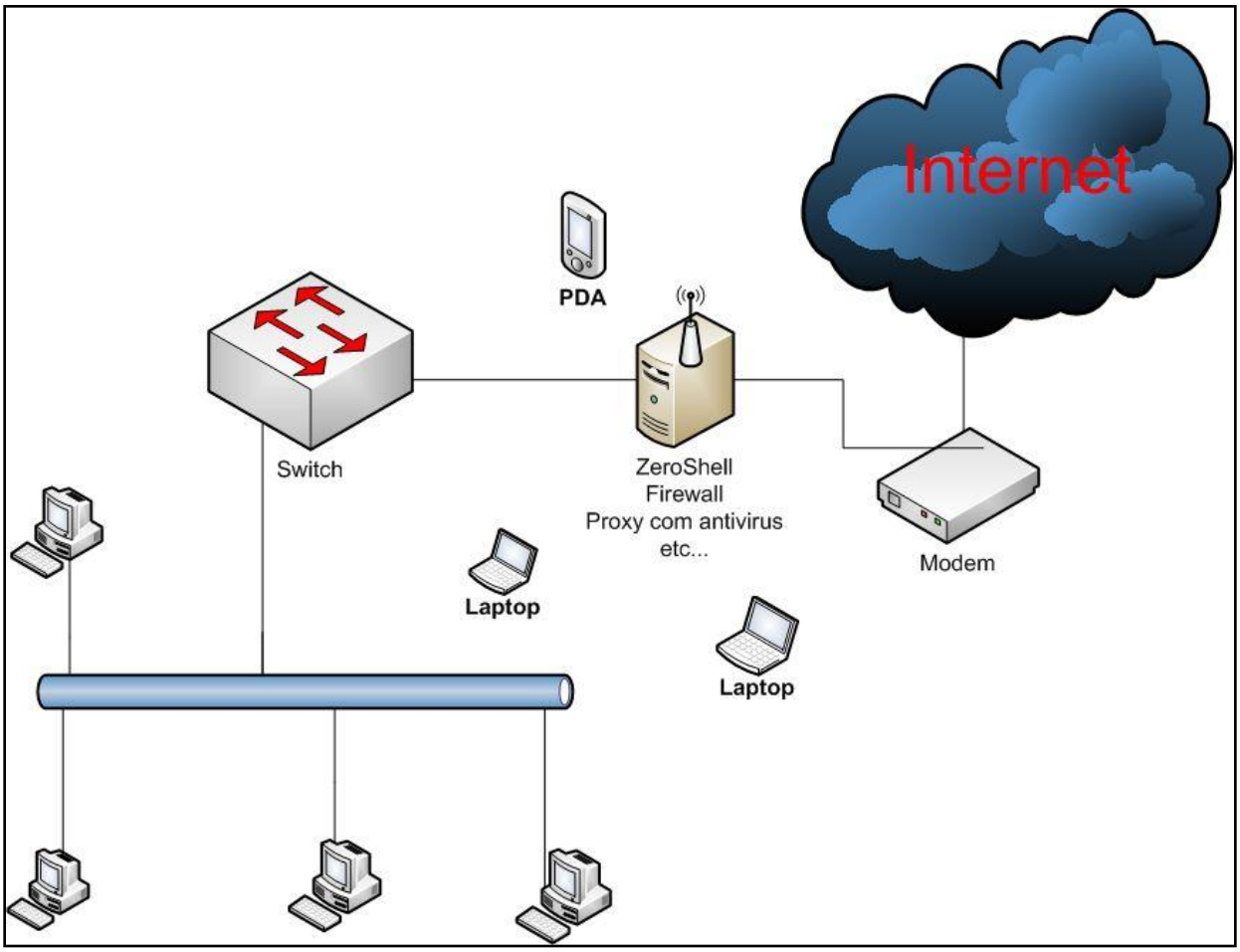


Figura 4: Rede CEAD com Wi-Fi

Na figura 4 é ilustrado o servidor ZeroShell provendo conexão com a Internet, para laptops e dispositivos móveis, via Wi-Fi para um laboratório de um polo.

2.6 ZEROSHELL

O ZeroShell (RICCIARD, 2009) é uma distribuição Linux, licenciado pela *GNU Public License* v2 (*GPL v2*), para servidores e provê os principais serviços requeridos em uma *Local Area Network* (LAN). Ele é disponibilizado em forma de *LiveCD* ou em imagem para *compact flash,* atualmente está na versão 1.0 beta 12, e ele pode ser administrado via interface web.

Como o ZeroShell é LiveCD para que as informações fiquem salvas e não sejam perdidas após o servidor desligar, o ZeroShell disponibiliza um mecanismo

chamado de *profile* o qual armazena todas as configurações e LOGs do sistema, para que quando o sistema seja reiniciado as informações não sejam perdidas.

O mecanismo de *profiles* possibilita que a configuração seja repassada entre vários servidores, independente da plataforma em que os sistemas estão instalados. Caso haja a necessidade de troca de *hardware* não é necessário fazer toda a configuração do novo servidor, basta instalar novamente o ZeroShell, e restaurar o *backup* da máquina antiga.

O ZeroShell foi desenvolvido por Fulvio Ricciard administrador de sistemas do Instituto Nacional de Física Nuclear (INFN) – Itália, em maio de 2009.

Esta distribuição disponibiliza de forma integrada vários serviços, e o trabalho em conjunto desses serviços visa fornecer uma maior segurança e qualidade de serviços para a rede.

Nesta distribuição a configuração, ativação/desativação e manutenção dos serviços é feita através de uma interface web disponibilizada pelo ZeroShell (como ilustrado na figura 5). Já as atualizações dos softwares utilizados pelo ZeroShell são realizadas automaticamente.

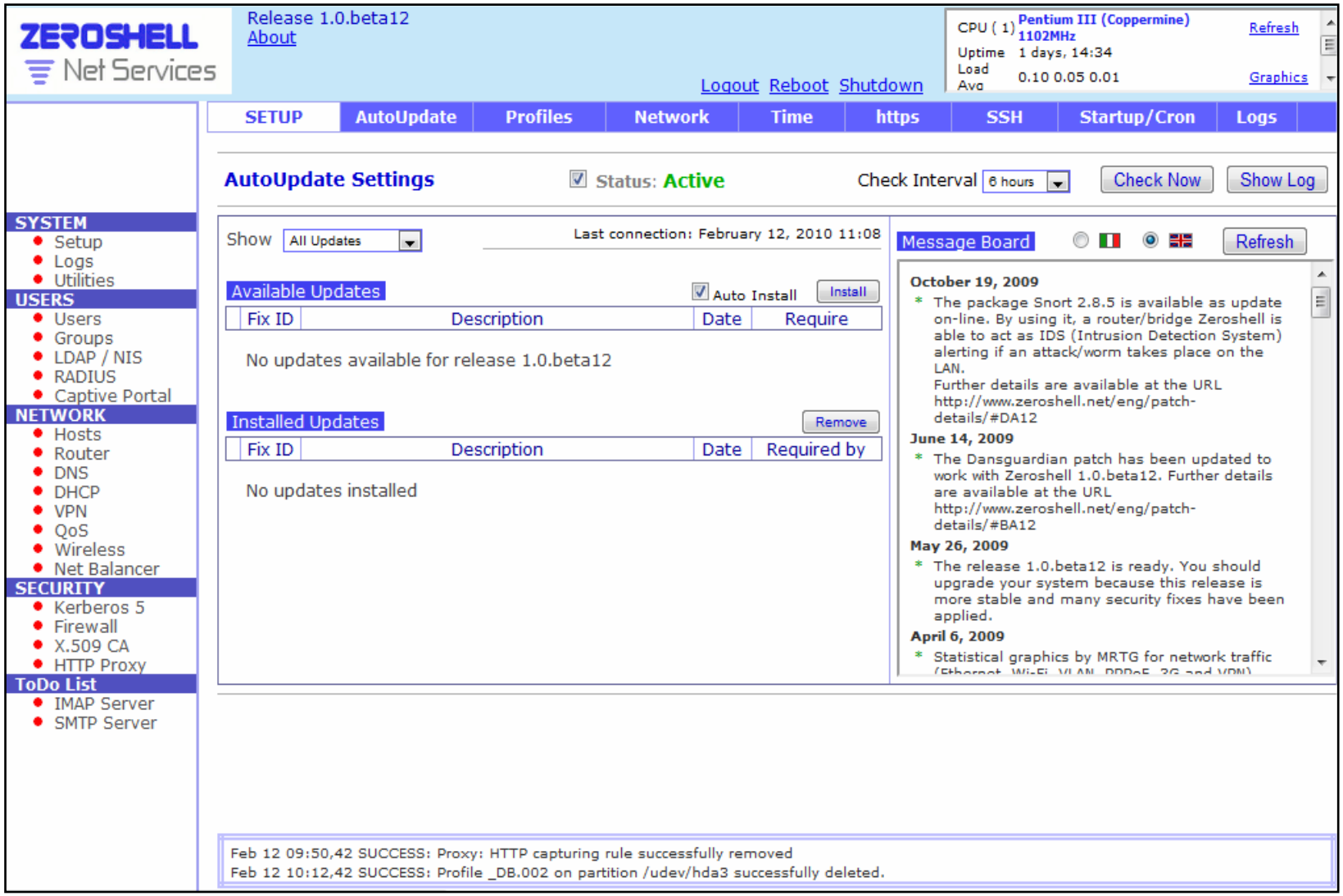


Figura 5: Página web de configuração do ZeroShell

3 INFRAESTRUTURA DE REDE DO CEAD

O CEAD, com sede no IFES campus Serra, é responsável pelos projetos de Educação a Distância (EaD) do IFES. Neste sentido, são oferecidos cursos em vários níveis: técnico, graduação, pós-graduação e formação continuada.

O CEAD oferece em parceria com as prefeituras do estado do Espírito Santo, por meio do sistema Universidade Aberta do Brasil (UAB), os cursos de Tecnologia em Análise e Desenvolvimento de Sistemas, Licenciatura em Informática e Técnico em Informática.

Mesmo o CEAD estando Localizado no IFES campus Serra, seu servidor foca localizado no IFES campus vitória, usufruindo assim da infra-estrutura de rede IFES para oferecer os cursos de EaD. O IFES campus Vitória possui dois links de 4 Mbps dedicados com a Internet, e um linkdedicado de 2Mbps com o IFES de vitória (como ilustrado na figura 6).

Com essa infraestrutura o CEAD fornece seus cursos, através do sistema UAB, comunicando-se com os polos de apoio presencial.

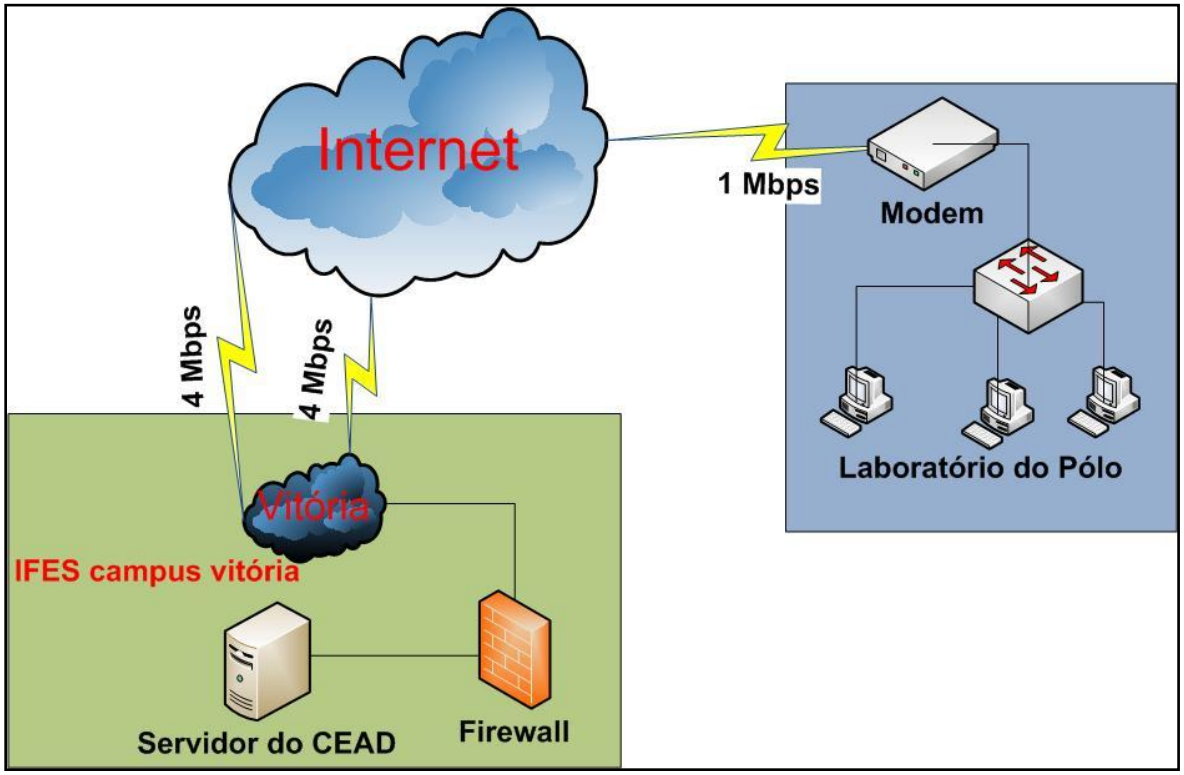


Figura 6: Rede do CEAD do IFES

3.1 O AMBIENTE DE UM POLO DE APOIO PRESENCIAL

Segundo a Universidade Aberta do Brasil -UAB- (UAB, 2010a) polos de apoio presencial:

> [...] São espaços físicos mantidos por municípios ou governos de estado que oferecem infraestrutura física, tecnológica e pedagógica para que os alunos possam acompanhar os cursos da UAB. [...]

Ou seja, é um espaço onde os alunos dos cursos de educação a distância podem realizar as atividades acadêmicas. Segundo a UAB (UAB, 2010b):

> [...] é crucial que o polo seja bem projetado para atender tanto às necessidades as instituições federais de ensino superior, quanto às necessidades dos estudantes, permitindo que todos os alunos tenham acesso aos meios modernos de

> informação e comunicação. [...]

Com isso a UAB (UAB, 2010a) definiu que um polo deve dispor de:

- Sala para Coordenação do Polo;
- Sala para Secretaria Acadêmica;
- Sala para Tutores Presenciais;
- Sala de aula típica;
- Sala para Professores;
- Sala de videoconferência;
- Auditório ou espaço adequado para reunião;
- Laboratório de informática;
- Biblioteca;

É no laboratório de informática que este trabalho tem foco, mas não deixando de lado a rede das outras dependências do polo. Os muitos polos de apoio presencial não possuem servidores. A topologia física e lógica da rede é em estrela, todos os computadores são ligados a um *switch* que por sua vez é ligado ao modem que possibilita o acesso à Internet, como representado na figura 7.

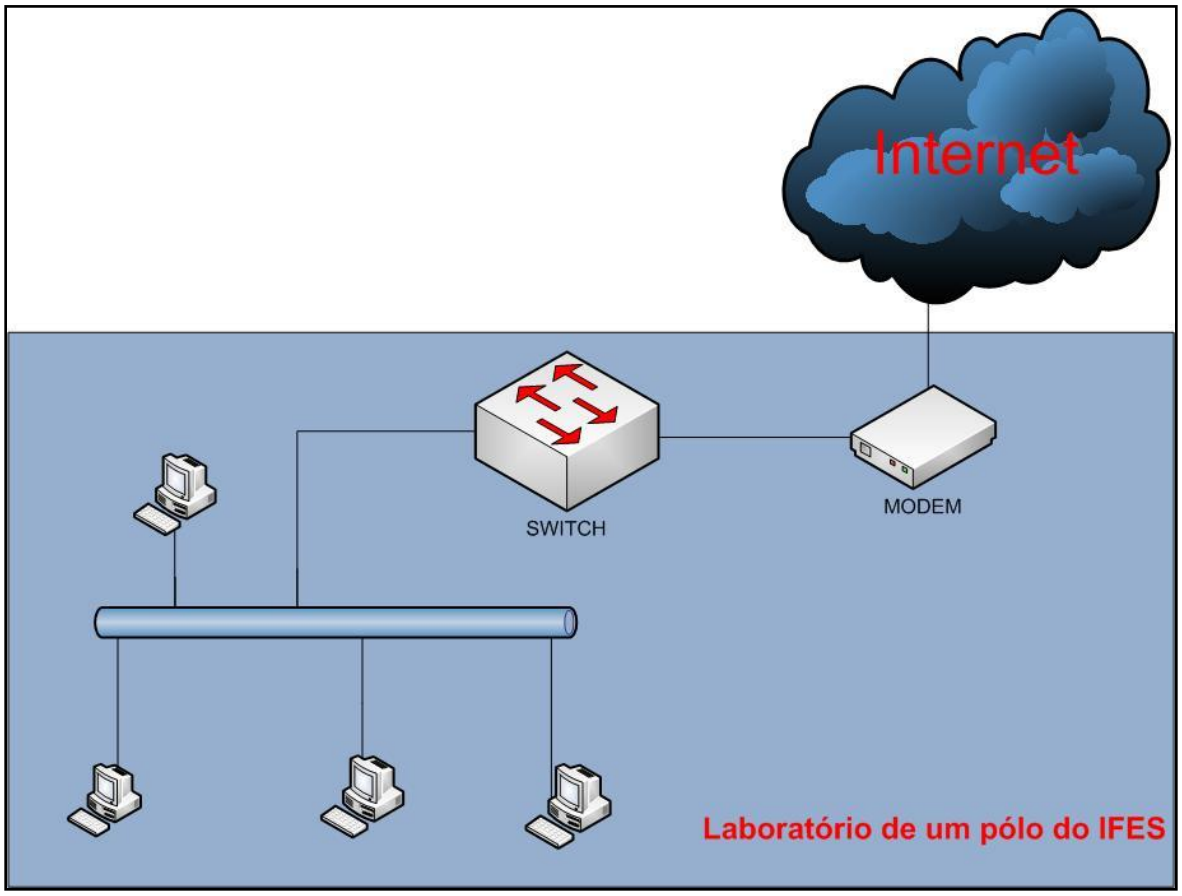


Figura 7: Rede do polo de apoio presencial

3.2 REQUISITOS DO SERVIDOR

Para que o polo possa atender às necessidades dos alunos ele deve possuir alguns serviços, para auxiliar no processo de ensino-aprendizagem

.

A rede interna de computadores dos polos de apoio presencial necessita de um servidor que atenda os seguintes requisitos de segurança, de desempenho e de *backup*.

Os requisitos de segurança são os seguintes:

- *Firewall*;
- *Proxy*;
- Antivírus;
- Autenticação para a rede sem-fio;

- Verificar todas as páginas web e as imagens nos formatos jpg, gif e png com o antivírus;
- Gerar LOG das páginas com vírus;
- Criar *Black List* de sites proibidos e *White List* para os sites permitidos.

Os requisitos de desempenho são os seguintes:

- O servidor deve funcionar, em uma máquina com no mínimo de 512 MB de memória RAM, 20 GB de HD e processador Pentium 3.

O requisito de *backup* é a disponibilidade de uma ferramenta que possibilite a cópia das configurações e do Logs do servidor sem que haja a necessidade de instalação da ferramenta na máquina, e que a operação seja executada em horário que a rede do polo de apoio presencial não esteja em atividade.

4 UMA PROPOSTA DE CONFIGURAÇÃO E SEUS BENEFICIOS

Este projeto propõe a utilização da distribuição ZeroShell que possui e integra grande parte dos serviços e dispositivos de segurança que o polo de apoio presencial necessita, além de ser de fácil configuração e instalação. Dentre esses serviços e dispositivos, estão os a seguir:

O *firewall* iptables contribuirá para a resolução dos problemas a seguir:

- Não permitir acesso não autorizado à rede interna do polo de apoio presencial;
- Prover o serviço de *firewall*;
- Serviço de NAT.

O Proxy HAVP contribuirá para a resolução dos problemas a seguir:

- Prover o serviço de *proxy*;
- Prover o serviço de antivírus;
- Verificar todas as páginas web e as imagens nos formatos jpg, gif e png com o antivírus;
- Gerar LOG das páginas com vírus;
- Criar *Black List* de sites proibidos e *White List* para os sites permitidos;

O dhcpserver contribuirá para atender a necessidade do servidor DHCP, já para prover a possibilidade da conexão Wi-Fi módulos kernel fornece esta possibilidade. Os módulos são os seguintes:

- *Wireless Tools*- Gerenciamento de interfaces *wireless*;
- *MadWIFI* - Módulo do kernel para placas de rede Wi-Fi;
- *WPA-Supplicant* - Autenticação WPA/WPA2 para clientes;
- *HostAP daemon* - Autenticação WPA/WPA2 para *access point*;

Para atender o requisito de *backup* o Zeroshell possui um sistema próprio conhecido como *profiles,* onde toda a configuração realizada no sistema, incluindo os LOGs, é salva nesse mecanismo. Para acessar esse mecanismo o Zeroshell fornece uma interface web que fornece a possibilidade de fazer uma cópia de *backup* desses *profiles*.

5 CONFIGURAÇÃO DE SERVIDOR E DOS SERVIÇOS

De acordo com os testes realizados durante alguns meses, o servidor ZeroShell funcionou em uma máquina de baixa capacidade de processamento e de armazenamento.

A máquina possuía uma configuração de 256MB de RAM, 20 GB de HD, sendo que menos de 1GB estava sendo ocupado, e um processador pentium 3. Com esta configuração o servidor ZeroShell estava provendo os serviços, protocolos e tecnologias de necessidade de um polo.

Com estes testes constatou-se que para a instalação e configuração do servidor ZeroShell primeiramente é necessário providenciar um computador com uma configuração mínima de:

- 256 MB de memória RAM;
- HD de no mínimo 5 GB;
- Processador Pentium 3;
- 2 Placas de rede;
- Leitor de cd;
- Entrada USB.

Para prover rede Wi-Fi pelo servidor ZeroShell é necessário adquirir uma placa de rede sem fio.

Com a posse de uma máquina com a configuração equivalente ou superior da citada anteriormente, pode-se fazer a instalação e a configuração do servidor ZeroShell.

5.1 INSTALAÇÃO DO *ZEROSHELL*

Para fazer a instalação primeiro é necessário fazer o *download* da imagem de instalação do ZeroShell no site http://www.zeroshell.net/eng/download/, como representado na figura 8, da versão mais atual do ZeroShell, que no caso é a versão 1.0 beta 12.

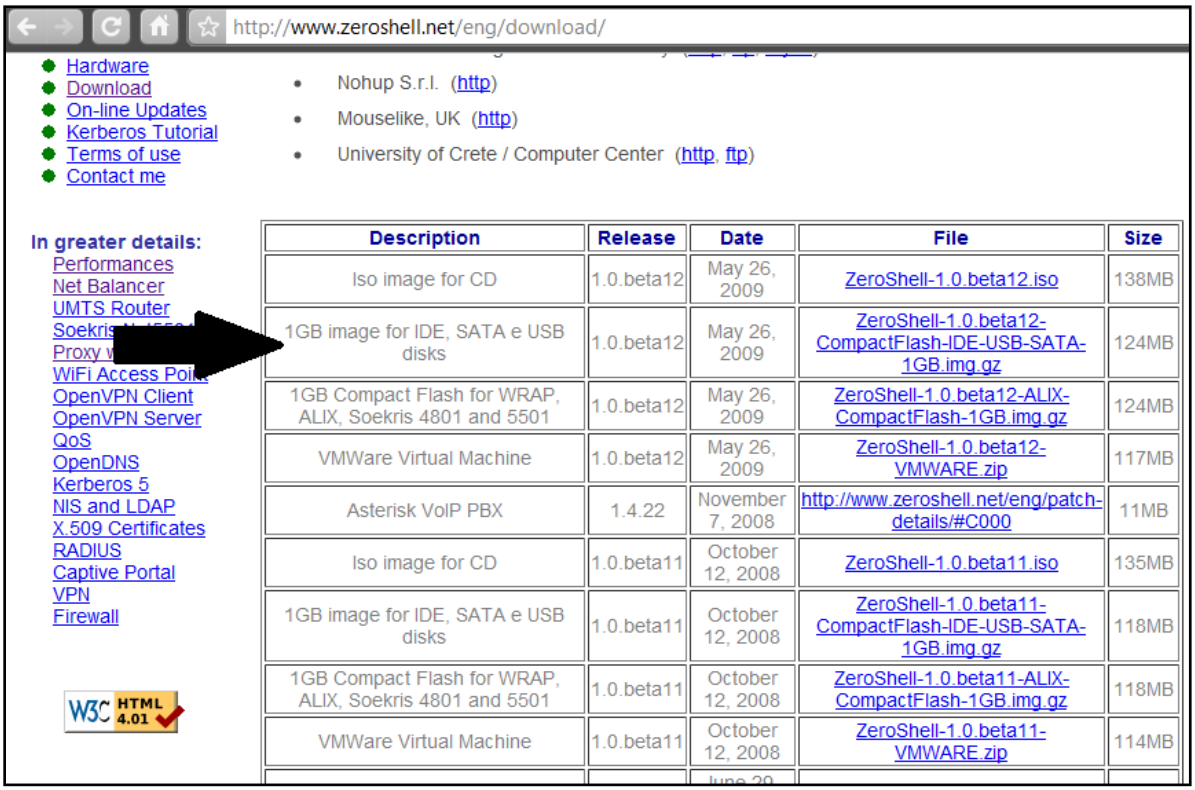


Figura 8: Página de *download* do ZeroShell.

Após fazer o download da imagem basta seguir os passos:

1. Coloquar a imagem em uma unidade de armazenamento USB (*pendrive*);
2. Iniciar o computador com qualquer liveCd de um SO Linux (ex: ZeroShell ou Ubuntu);
3. Abrir o Shell (console de comandos) (no caso do ubuntu aplicações>acessórios>console já no caso do ZeroShell aperte o atalho 'S');
4. Digitar o comando **fdisk –l** (Como representado na figura 9);
   No exemplo o HD é o **/dev/hda**, e o *pendrive* é o **/dev/sda1**.
5. Com isso é necessário montar o *pendrive*, para isso cria-se uma pasta no diretório **/mnt** com o nome **pendrive** com o seguinte comando.
   ***mkdir /mnt/pendrive*.**

6. Com a pasta criada, monta-se o *pendrive* com o seguinte comando:
   mount /dev/sda1 /mnt/pendrive

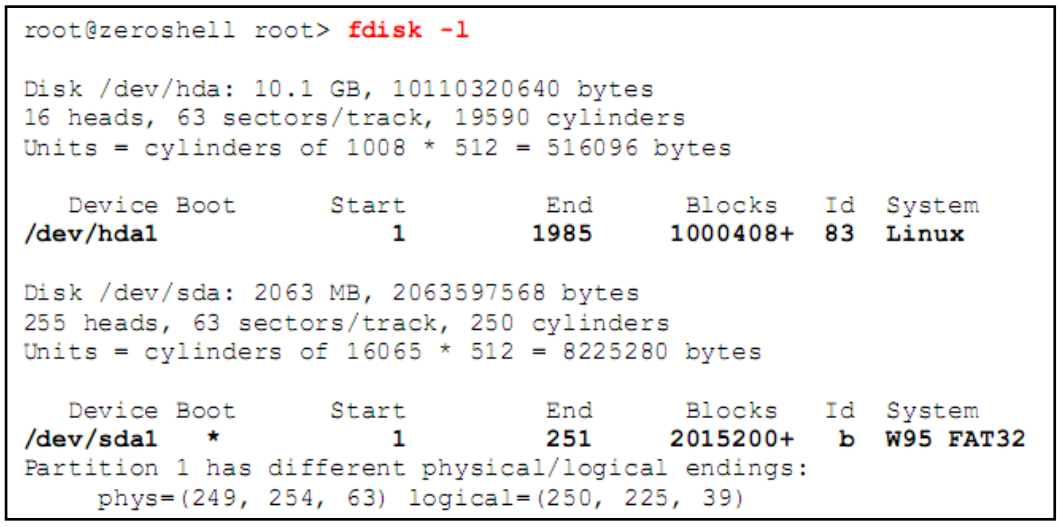


Figura 9: resultado do comando fdisk -l

7. Com o *pendrive* montado, tudo está pronto para a instalação, para isso basta digitar o comando:
   gunzip -c /mnt/pendrive/zeroshell.img.gz>/dev/hda

Aguarda-se descompactar, e então se reinicia o sistema, com o comando **reboot**. Retira-se o cd e o sistema iniciará pelo HD.

5.2 CONFIGURAÇÃO DA INTERFACE DE REDE DO ZEROSHELL

Com o sistema instalado, é necessário configurar a interface de rede do ZeroShell e acessar sua interface Web para poder configurar os serviços.

Antes de configurar a interface de rede do ZeroShell, por motivo de segurança, é necessário alterar a senha padrão do administrador. Para isso no menu inicial digita-se o atalho ‘P’ e digite a nova senha de administrador.

Para efetuar a configuração da interface de rede, no menu principal do ZeroShell digita-se o atalho ‘I’ , para configurar a interface, aparecerá um novo menu, nesse menu aperte o atalho ‘A’ que irá direcionar para menus questionando sobre a

conexão que deseja-se configurar, para melhor entendimento será utilizado a rede ilustrada na figura 3.

O primeiro menu questiona qual interface deseja-se configurar, no ZeroShell as interfaces são representadas com dois números ao invés de um somente, por exemplo, eth00 ou eth01 e assim por diante. Escolhe-se a interface digitando seu respectivo identificador e aperta-se Enter. Em seqüência devem-se inserir os dados, iniciando pelo endereço IP (no exemplo 192.168.1.1), depois pela mascara (no exemplo 255.255.255.0).

Com a interface de rede configurada, o próximo passo é a configuração dos serviços que serão oferecidos pelo ZeroShell. Para configurá-los é necessário acessar sua interface web, por um computador que está na mesma rede que ele. Digita-se o endereço IP do servidor ZeroShell (no exemplo 192.168.1.1) na barra de endereços do navegador Web, será apresentada a página de login para acessar o ZeroShell. Entra-se com o *Login* (admin) e Senha.

Inicialmente criaremos um *profile* para salvar as configurações feitas no servidor.

5.3 CRIAÇÃO DE UM *PROFILE*

Como visto anteriormente o *profile* é um mecanismo do ZeroShell que armazena as configurações efetuadas no servidor.

Para criar um *profile* acessa-se no menu lateral esquerdo *System>Setup*, com isso a página é recarregada e no menu horizontal superior, acessa-se *Profile*. A página será alterada para a página de gerenciamento de profiles (como ilustrado na figura 10).

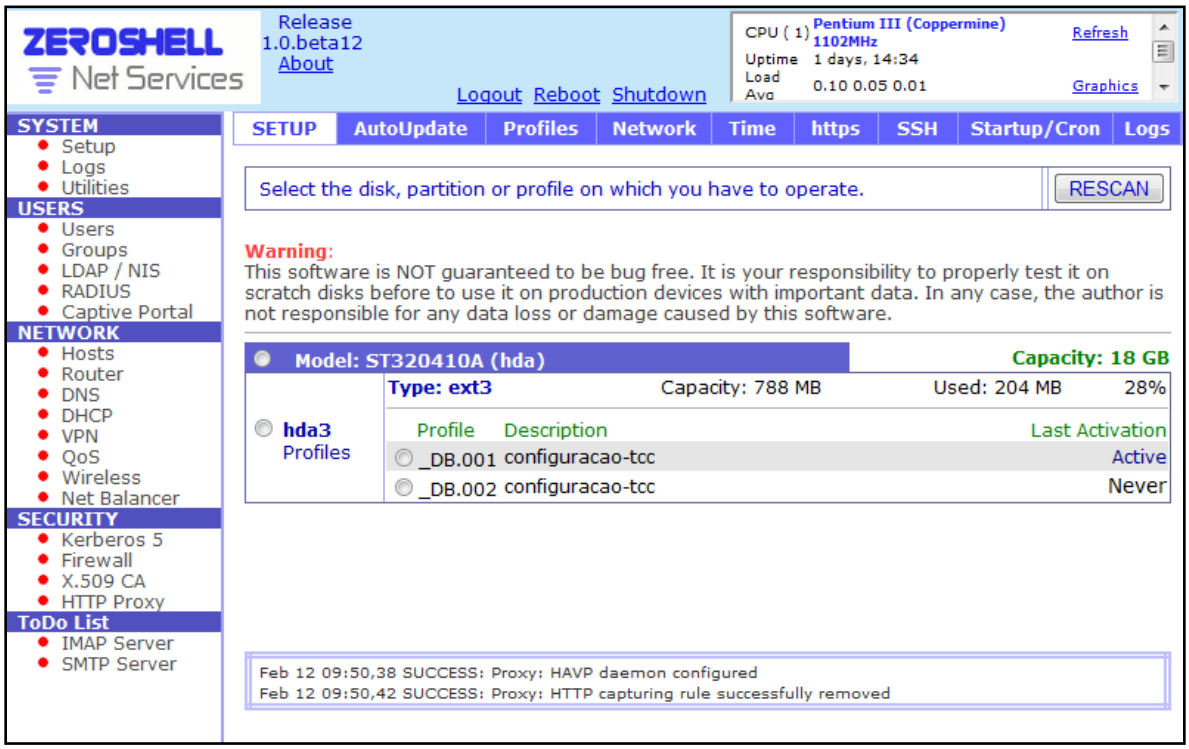


Figura 10: Página de gerenciamento de *profiles*

Nesta página serão apresentados os dispositivos de armazenamento da máquina, escolhe-se um onde se deseja armazenar suas informações de configuração. Ao selecionar o dispositivo de armazenamento será mostrado um novo menu com botões acima dos dispositivos de armazenamento (Como representado na figura 11), então clicando no botão "*Create Profile"* será aberta uma nova janela, pedindo as informações do *profile* (como ilustrado na figura 12) é necessário alterar somente o campo "*Description*" e o campo "*Admin password*". Depois de preenchidos os campos, clica-se no botão "*create*", no canto superior direito da página, e o *profile* estará criado, basta ativá-lo, selecionando-o e clicando no botão "*active*" no menu superior da página, para que salve todas as configurações.

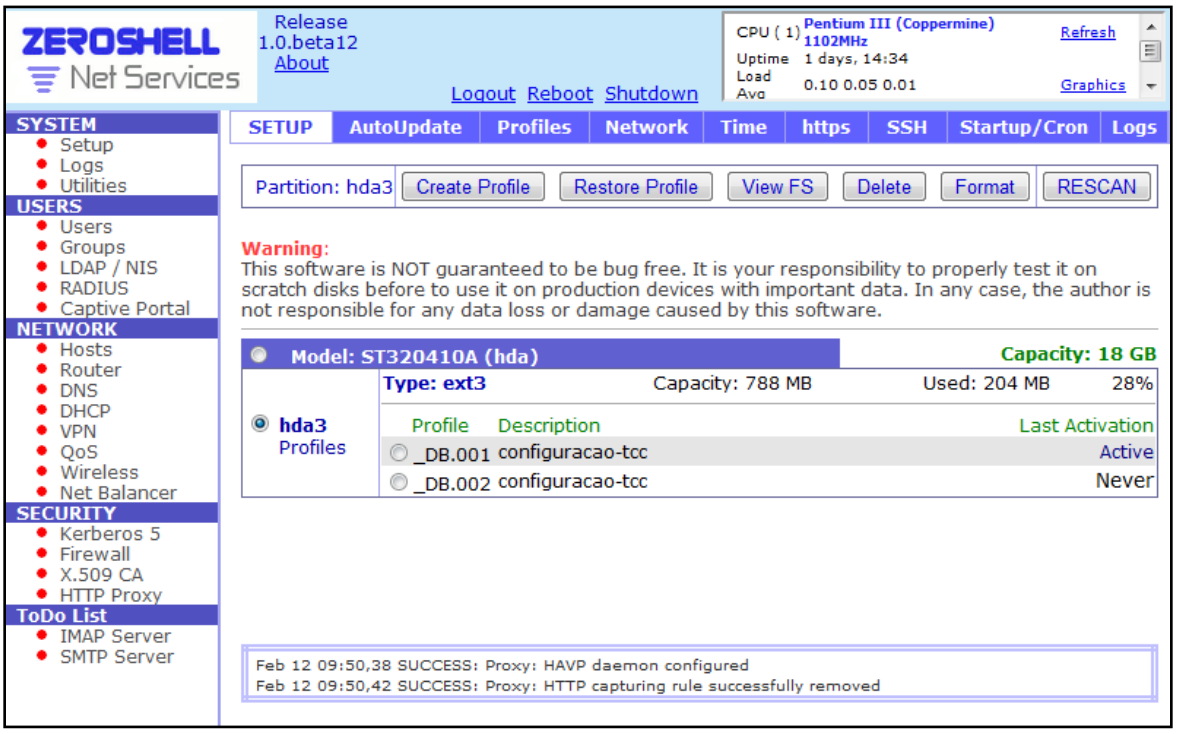


Figura 11: página de gerenciamento de *profiles*, criando *profile*

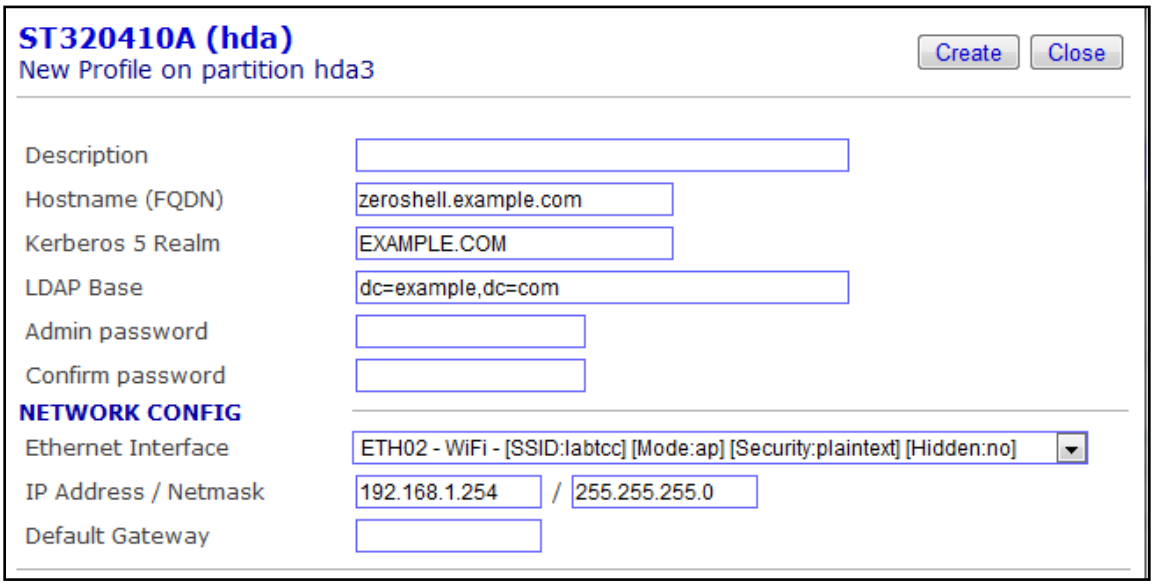


Figura 12: Página de criação de novo *profile*

Com isso pode-se dar inicio a configuração dos serviços que serão oferecidos, pois as configurações serão todas salvas.

5.4 COFIGURAÇÃO DO DHCP

Para configurar o DHCP acessa-se o menu lateral esquerdo *Network >DHCP*. Será redirecionado para a página de configuração do DHCP (como ilustrado na figura 13).

Na tela de configuração do DHCP, na divisão *Dynamic IP Configuration*, configura-se as faixas de IP que serão distribuídas, na primeira coluna digita-se o endereço IP inicial que será distribuído e na segunda coluna digita-se o endereço IP final que será distribuído, para a sub-rede selecionada no item *subnet*.

Já no canto direito da página na divisão *Subnet Options*, configura-se as informações que serão repassadas aos clientes DHCP, como rota padrão (*default gateway*), servidor DNS entre outros.

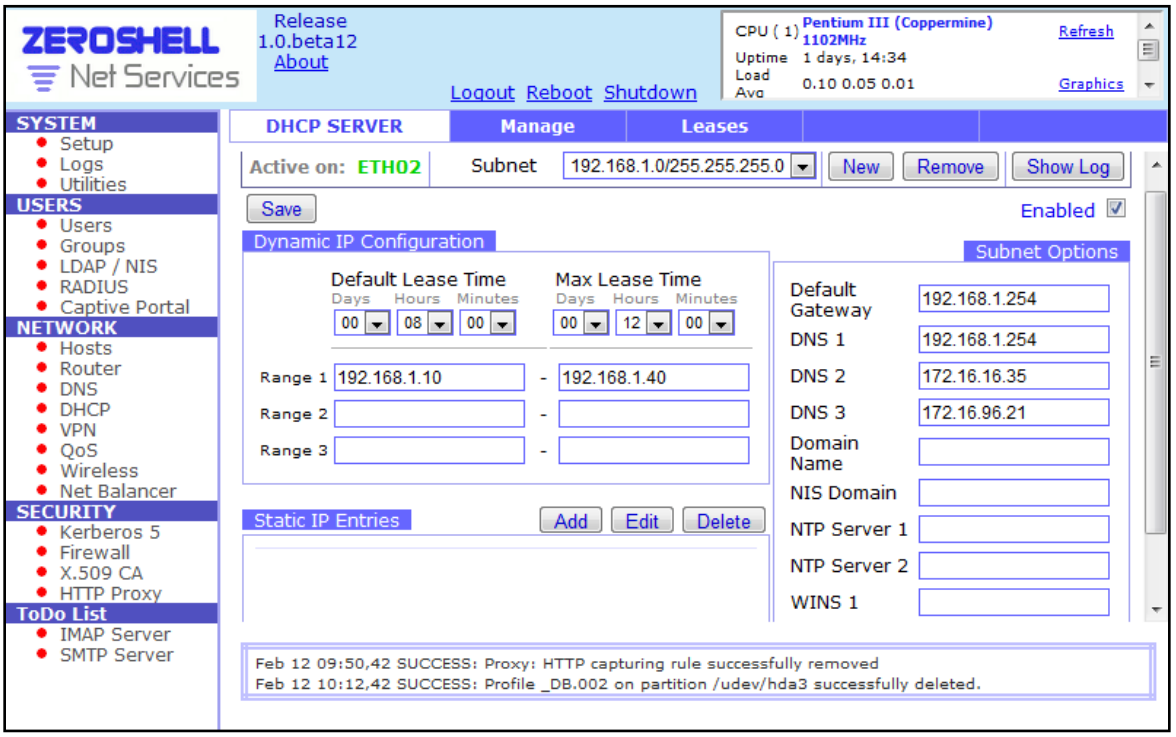


Figura 13: Página de configuração do DHCP

Após o termino da configuração do DHCP, deve-se salvar as configurações, clicando no botão “*save*” no canto superior esquerdo da tela.

5.4.1 CONFIGURAÇÃO DO DNS

Caso o servidor ZeroShell não irá trabalhar como DNS é necessário redirecionar

as requisições dns dos clientes para o servidor DNS. Para fazer esse redirecionamento acessa-se no menu vertical esquerdo *Network* > *DNS,* a seguir no menu horizontal superior na opção "*Forwarders"* , aparecerá uma nova janela (como ilustrado na figura 14), nela há dois campos, o primeiro é o domínio da requisição, e o segundo para onde irá encaminhar a requisição. Caso o servidor DNS seja outra máquina, digita-se **ANY** no primeiro campo, e no segundo campo o endereço do servidor DNS, e clica-se no botão "add".

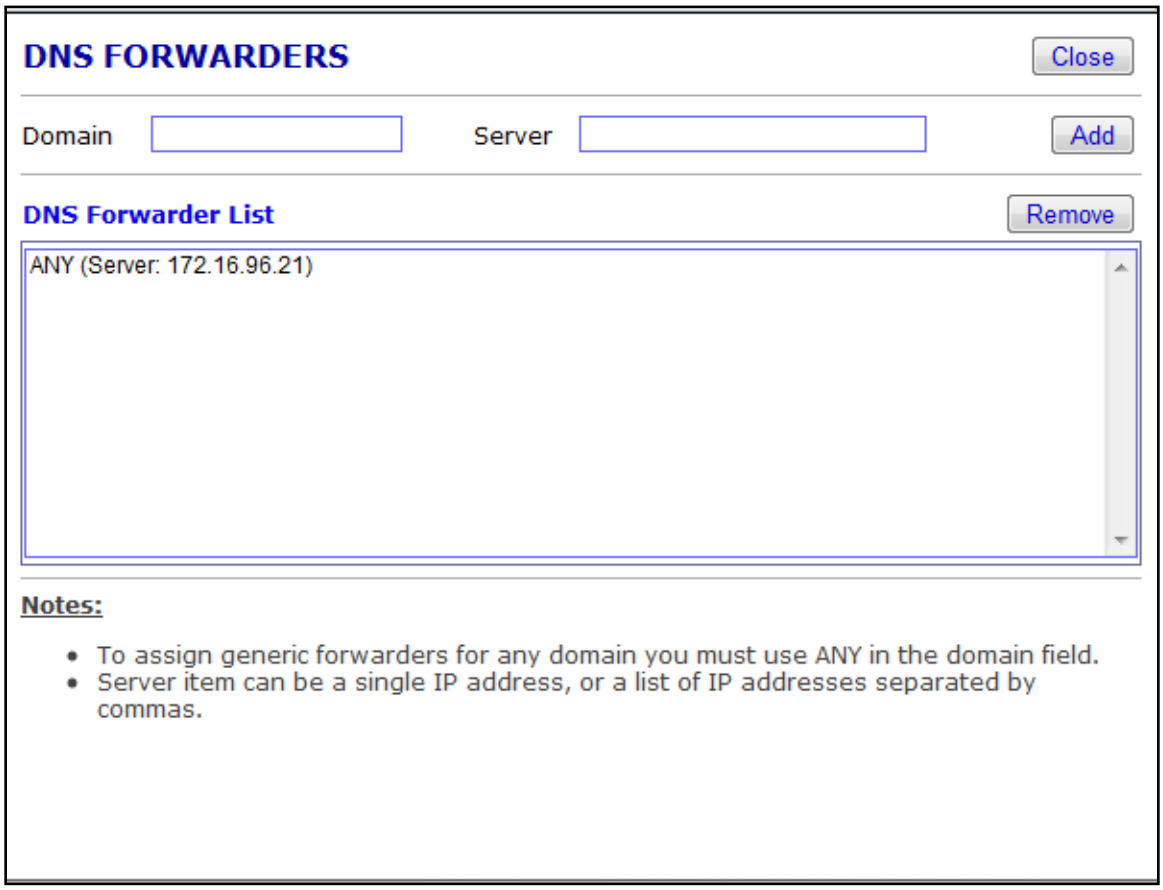


Figura 14: página de redirecionamento DNS

5.5 CONFIGURAÇÃO DO NAT

Para configurar o NAT acessa-se no menu vertical esquerdo *Network* > *Router*, será redirecionado para a página de configuração das funcionalidades de roteador do ZeroShell, no menu superior acessa-se NAT, que redirecionará para a página de gerenciamento do NAT (Ilustrado na figura 15).

Considerando-se que a interface que está ligada a Internet é a eth01, ativa-se o

NAT para essa interface. Com isso o NAT já estará funcionando.

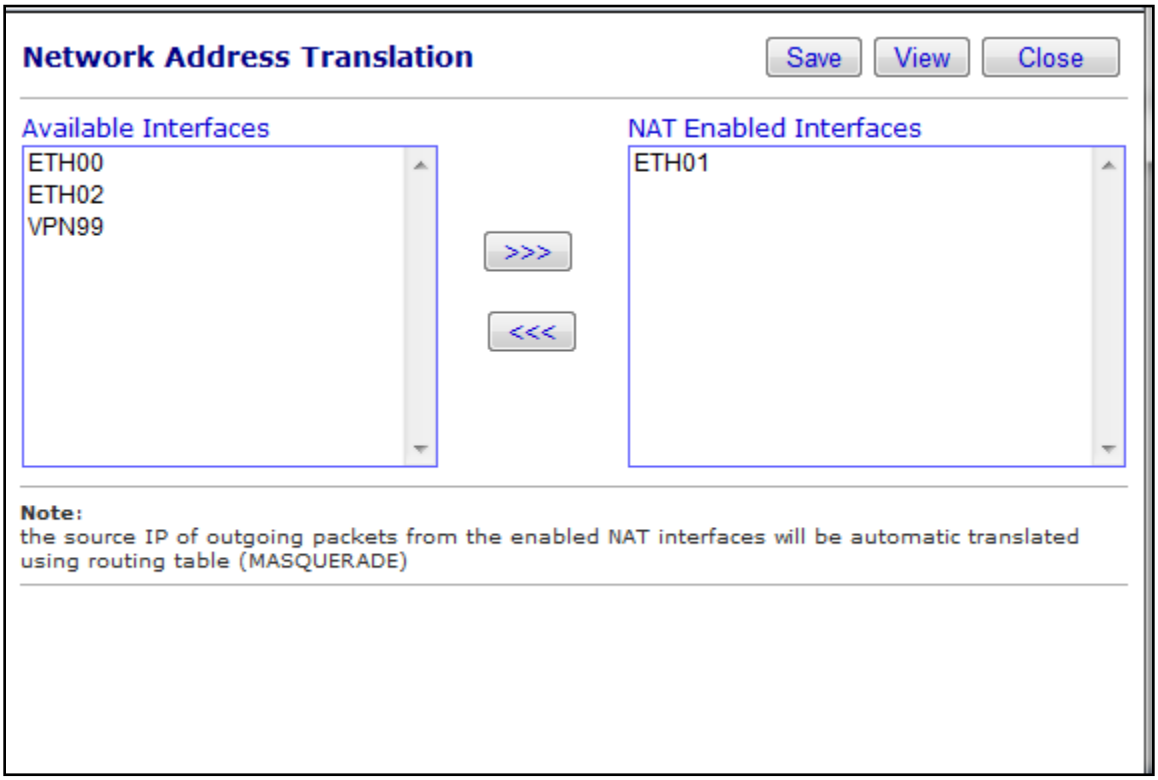


Figura 15: Página de configuração do NAT

5.6 CONFIGURAÇÃO DO *PROXY* COM ANTIVÍRUS

Para configurar o Proxy com o antivírus acessa-se no menu vertical esquerdo *Security* > *HTTP Proxy*, será redirecionado para a página de gerenciamento do Proxy (como ilustrado na figura 16), nesta página selecione o campo "*Enabled*" para habilitar esse serviço.

Com isso configura-se o *Black List*, que é a lista de sites que não poderão ser acessados através dessa rede, e o *White List*, que é a lista de sites que podem ser acessados. Estas configurações se encontram no canto inferior direito da página, na divisão "*URL Managment"*, clicando no botão "manage" abrirá uma janela (como ilustrado na figura 17). Nesta janela adiciona-se os endereços dos sites que se deseja bloquear, no caso do *Black List*, ou liberar, no caso do *White List*.

Para que o *proxy* bloqueie todas as páginas do site é necessário utilizar o caractere reservado ***** , ele representa “tudo”. Por exemplo, se for necessário bloquear o site do terra, caso seja utilizado somente **www.terra.com.br**, ele bloqueará somente a página inicial desse site, já se utilizar **www.terra.com.br/*** ele bloqueará todas as páginas do terra, mas caso haja outros destinos além do **www**, ele não bloqueará, por exemplo **tecnologia.terra.com.br**, será liberado, para bloqueá-lo utiliza-se ***.terra.com.br/***.

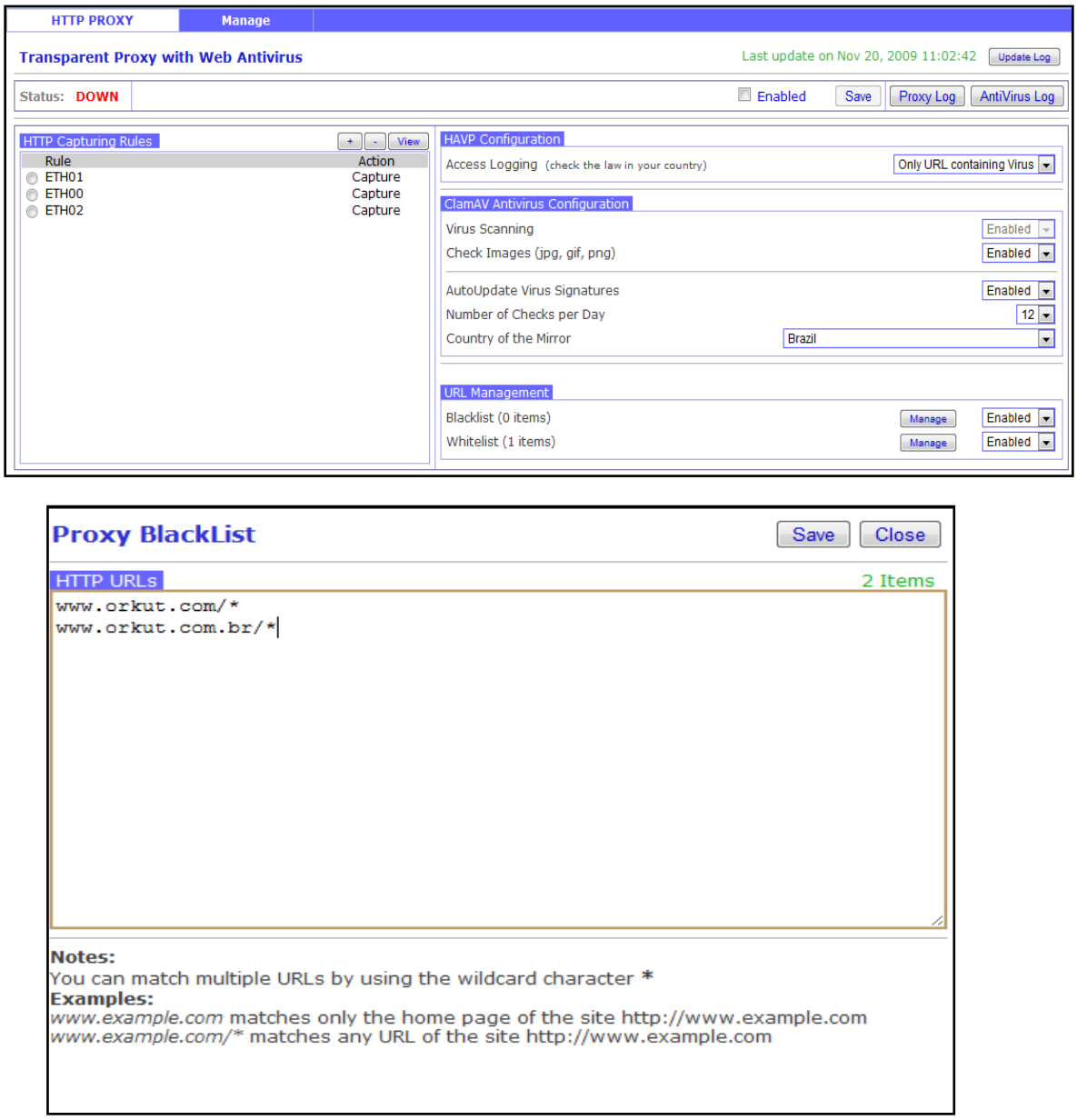


Figura 16: Página de gerenciamento do Proxy

Figura 17: Página de configuração de *Black List*

Após criar as lista de todos os sites que se deseja bloquear clica-se no botão "*save*" no canto superior direito da página.

Com os Black e White List criados, agora se configura para quais interfaces essas regras irão ser aplicadas. Para isso na divisão "*HTTP Capturing Rules*", clica-se no botão com o símbolo de "+" e será aberta uma página (como representada na figura 18), no campo "Action" seleciona-se "*Capture Request*", no campo "*Source Interface*" seleciona-se a interface de onde os dados vão ser capturados, no caso a interface interna, no campo "Source IP" o endereço IP da máquina de origem e no campo "*Destination IP*" o endereço IP da máquina de destino, caso não preencha esse campo a regra valerá para todas as máquinas da rede. Após os campos preenchidos clica-se no botão "*Save*".

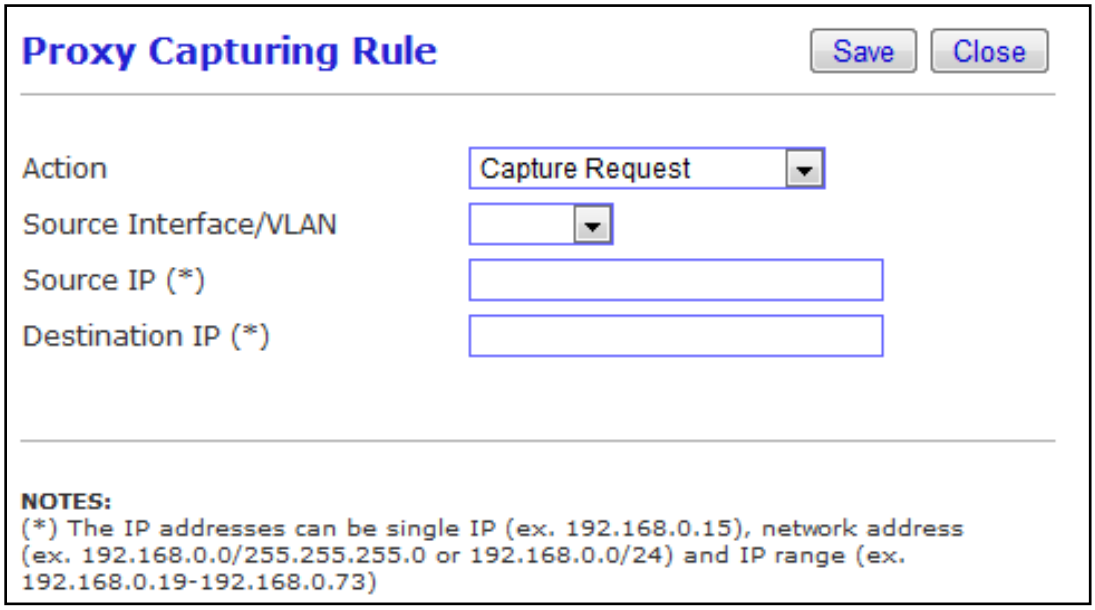


Figura 18: Página de gerenciamento de interfaces de captura do Proxy

Após essas configurações ativa-se o antivirus, na divisão "*ClamAV Antivirus Configuration*", ativa-se o "*Virus Scanning*" e o "*Check Images (jpg, gif, png)"* e o "*AutoUpdate Virus Signatures*". Após todas as configurações clica-se no botão "*Save*" no canto superior da página.

5.7 CONFIGURAÇÃO DA REDE Wi-Fi

Para configurar a rede Wi-Fi, na versão mais atual, ainda não possui a possibilidade da sua configuração via interface web. Então para configurar a rede Wi-Fi, no menu principal do ZeroShell digite o atalho “W”, o menu será alterado para o menu de gerenciamento das conexões Wi-Fi. Neste menu digita-se o atalho “N” para criar uma nova rede. Será questionado sobre várias dados sobre a conexão, inicialmente será perguntado sobre a interface que será utilizada, escolha a interface, exemplo (wifi0), a próxima questão é sobre o modo de atuação da placa, 1 para modo Access point, e 2 para modo cliente, como deseja-se criar uma rede sem fio, a opção a se escolher é 1. A próxima questão é sobre o SSID (nome) da rede, digita-se o nome desejado. A próxima questão é sobre a intenção ou não de esconder o SSID, digite Yes para esconder e No, para não esconder. A seguir a questão é sobre a utilização do sistema WDS[1], digita-se ***yes*** para utilizar, ou ***no*** para não utilizar. Depois disso a questão é sobre a forma de criptografia, as opções são:

1. Texto Plano (Sem criptografia);
2. WPA-EAP/RSN/802.1X+WEP (Criptografia, com autenticação no servidor RADIUS);
3. WPA-PSK (Criptografia com chave compartilhada);
4. WEP.

Este trabalho propõe a utilização da criptografia WPA-PSK, por ser mais seguro (procurar referencia) que o WEP, e por não ter sido implantado o servidor RADIUS. Em seguida digita-se a chave que se deseja utilizar.

Com a rede Wi-Fi criada, agora se adiciona um endereço IP para essa interface, no menu principal do ZeroShell, digita-se o atalho ‘I’, que irá redirecionar para a página de configurações de redes, para adicionar um endereço IP a essa interface, basta seguir os mesmos passos citados no tópico 5.2.

---

[1] WDS – *Wireless Distribution System*, serve para um sistema que permite a interconexão de *access points* sem a utilização de cabos ou fios.

5.8 CONFIGURAÇÃO DO *FIREWALL*

Para configurar o *firewall* no ZeroShell existem dois caminhos, o primeiro é pela interface gráfica, disponibilizada pelo ZeroShell para criar regras de *firewall,* a outra forma é criar os comandos manualmente, este documento irá mostrar como elaborar as regras das duas maneiras.

Primeiramente pelo modo dos comandos, para isso na página web do ZeroShell no menu vertical esquerdo acessa-se *System* > *Setup* a página será redirecionada para a página inicial da configuração do ZeroShell, no menu superior acessa-se "*Startup/Cron*" irá abrir uma nova janela (como ilustrado na figura 19). Nessa janela na parte superior a um objeto de seleção, seleciona-se "*Firewall*". Nesta janela de acordo com a cadeia se insere as regras do *firewall iptables*.

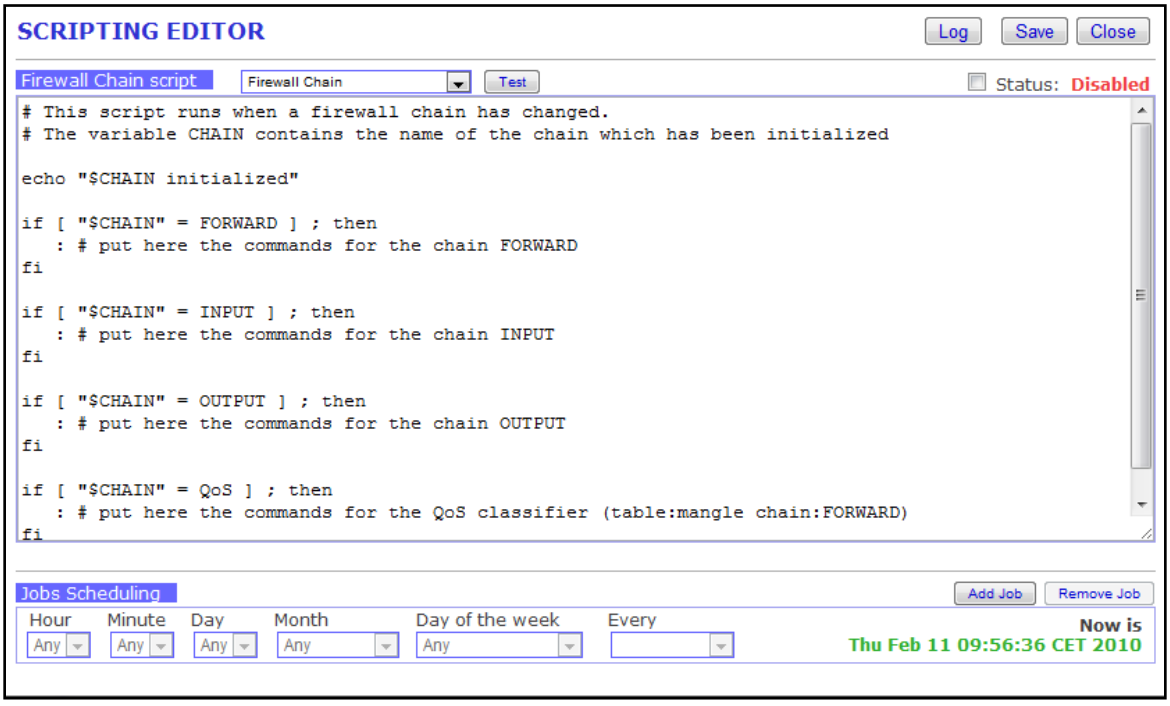


Figura 19: Página de criação de regras via comandos para o *firewall* iptables

O outro modo para criar as regras do firewall *iptables* é acessando no menu vertical esquerdo *Security* > *Firewall*, será redirecionado para a página de gerência do firewall. Nesta página podem-se criar as regras de firewall (como ilustrado na figura 20).

Para isto no menu superior há um objeto de seleção onde está escrito "*Aply to*", ou

seja, para quais pacotes aquela regra será aplicada (como ilustrado na figura 21), há três opções, são elas:

- *Routed and Bridged Packets* (Pacotes roteados e que passam pelo modo *bridge*);
- *Routed Packets Only* (Pacotes roteados somente);
- *Bridged Packets Only* (Pacotes do modo *bridge* somente).

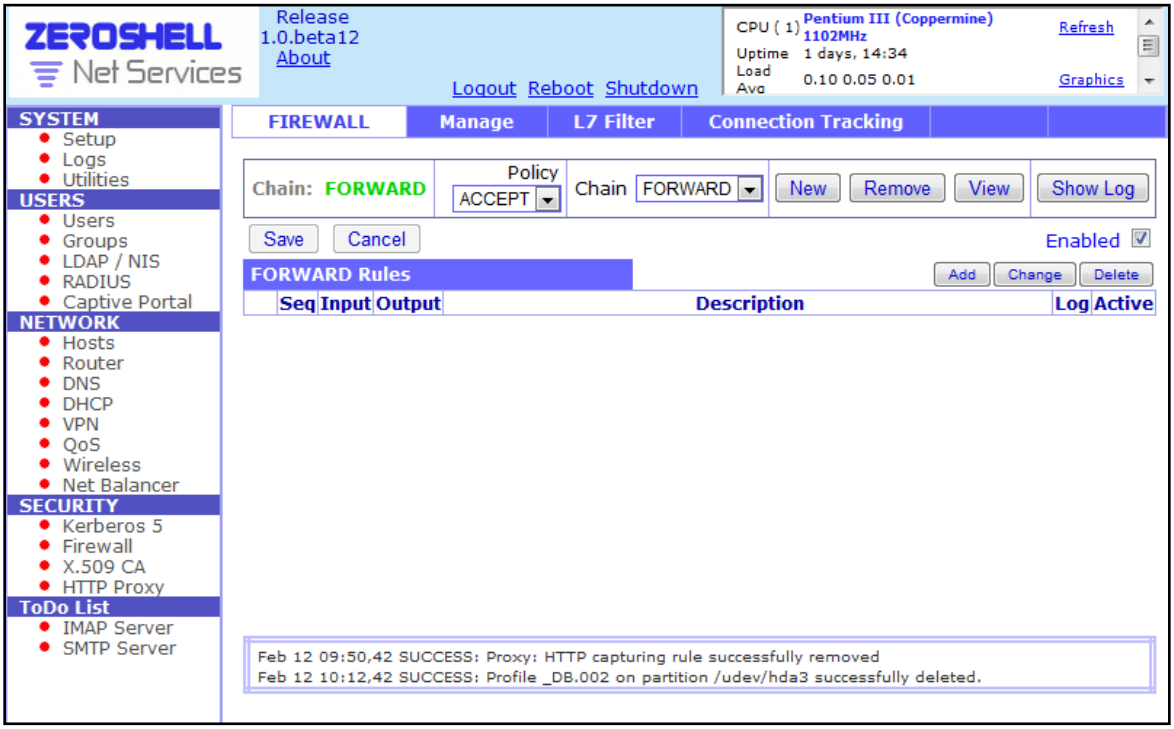


Figura 20: Página de gerenciamento do *firewall*

Após isso se escolhe a cadeia (*Chain*) a qual a regra, que será criada, pertencerá e também qual é a regra padrão (*Policy*), ou libera tudo ou bloqueia tudo (*accept* ou *drop*). Selecionando a cadeia e a regra padrão, clica-se no botão "*add*" para adicionar uma regra na cadeia. Com isso, será aberta uma nova janela (como ilustrado na figura 21), onde se seleciona, dependendo da cadeia, os seguintes itens:

- A interface de entrada (*Input*);
- A interface de saída (*Output*);
- O endereço IP de origem (*Source IP*);

- O endereço IP de destino (*Destination IP*);
- O protocolo que deseja tratar na regra (*Protocol Matching*);

A seguir seleciona-se, no campo "***connection state",*** os estados da conexão que a regra será aplicada, depois no campo "*Iptables parameters*" adiciona-se parâmetros do iptables, a seguir informa-se quais os dias e horários que a regra será aplicada, no campo "*Time Matching*", também há a possibilidade de selecionar alguns protocolos da camada de aplicação, através do campo *Layer* 7 *Filters* (filtros da camada 7), entre outros campos.

Preenchem-se todos os campos necessários para a regra de *firewall* que se deseja, e no final seleciona se deseja bloquear ou liberar, no campo "*Action*", com as opções *DROP*, *ACCEPT* ou *REJECT*.

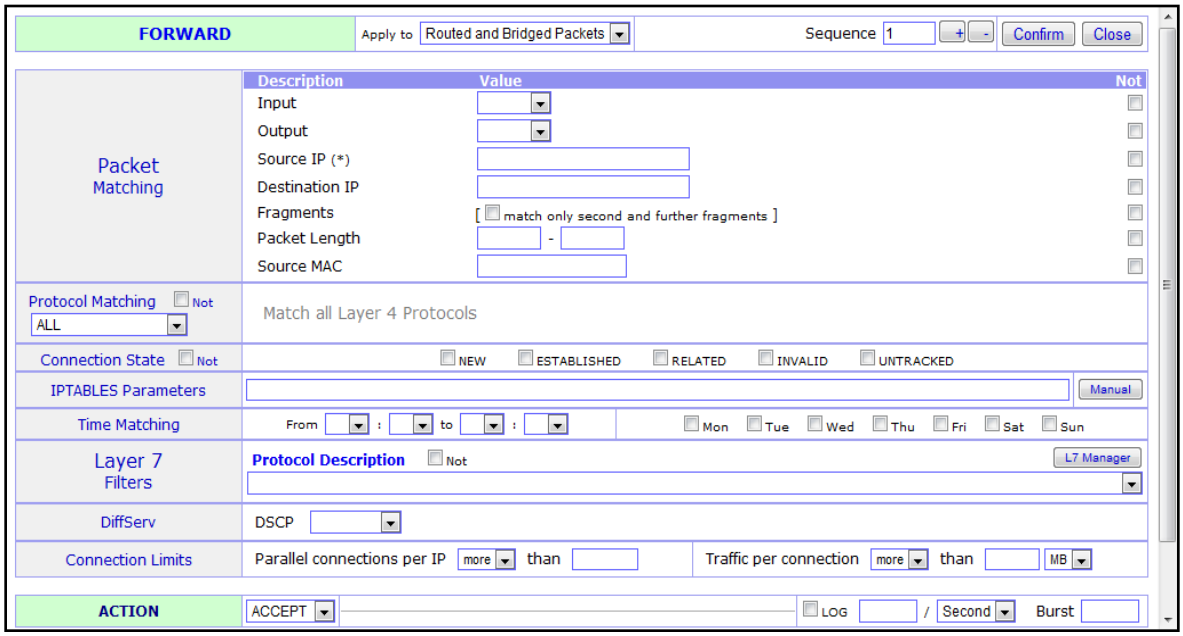


Figura 21: Página de criação de regra do *firewall iptables* via interface gráfica

5.9 BACKUP

5.9.1 REALIZAR *BACKUP*

Para realizar o *backup* das configurações do ZeroShell existem dois modos, o

primeiro é fazendo o *download* do backup para outra máquina e o outro modo é fazendo uma cópia do *backup* para um *pendrive*.

Caso a escolha seja pelo download, na página Web do ZeroShell no menu esquerdo acessa-se *System* > *Setup*, a página será alterada para a página principal do ZeroShell, no menu horizontal superior acessa-se *Profiles*, será redirecionado para a página de gerenciamento de *profiles* (como ilustrado na figura 22). Então se seleciona o *profile* que se deseja realizar o *backup*, com isso aparecerá botões relacionados ao *profile*, um deles é o de backup. Clicando no botão de *backup*, será efetuado o *download* dos dados comprimidos para a máquina que está acessando.

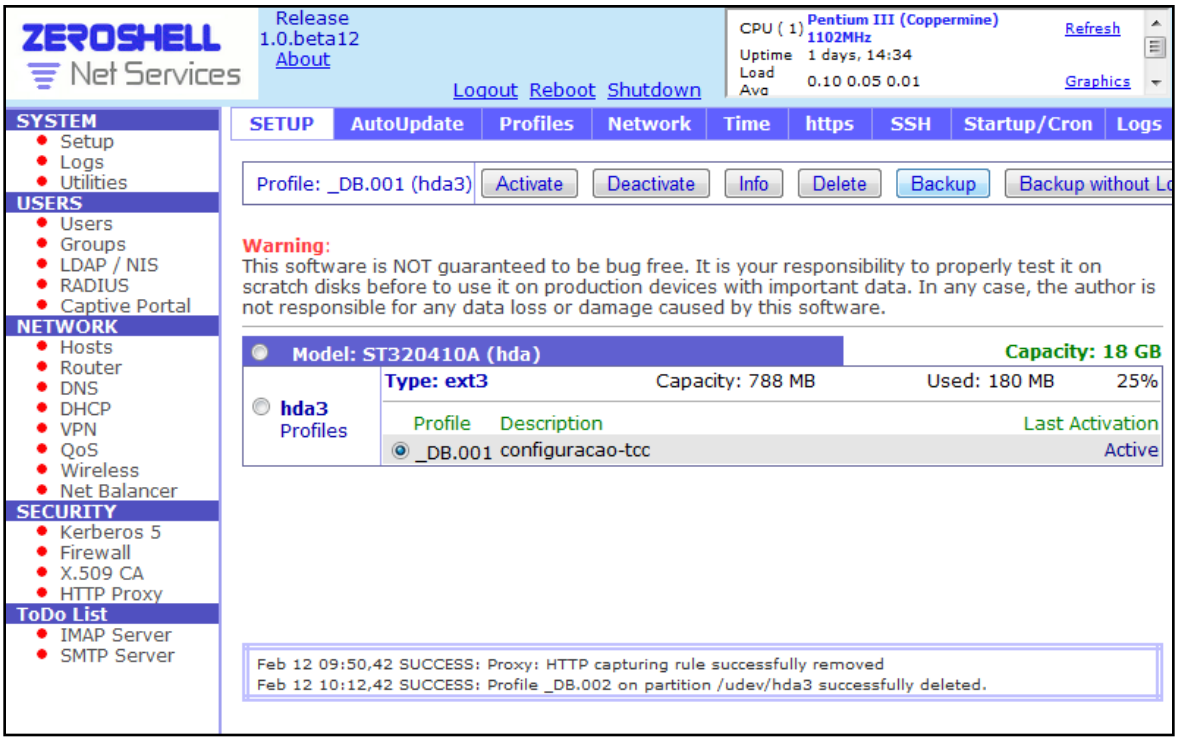


Figura 22: Página de *backup* de *profile*

Caso a escolha seja copiar para o *pendrive*, basta ligar o *pendrive* no servidor ZeroShell e então na mesma página acima clica-se no botão “*copy*”, então os dados serão copiados para o pendrive.

Observando que para realizar o *backup* o *profile* não pode estar sendo utilizado no

momento, caso só possua este *profile*, desativa-se o *profile,* então a máquina irá reiniciar, realiza-se o procedimento do tópico 5.2, e acessando a interface web, e realiza-se o *backup* do *profile*. A seguir o ativa-se novamente o *profile*.

5.9.2 RESTAURAR O *BACKUP*

Para restaurar um backup, na mesma página acessada no tópico 5.9.1, seleciona-se o destino da restauração (no caso hda3), irá aparecer um botão "*Restore Profile*", clicando neste botão irá abrir outra janela (como ilustrado na figura 23). Clica-se no botão "Escolher arquivo", então selecione o arquivo de *backup* e mandar restaurar. Após a restauração o arquivo estará pronto para ser ativado e utilizado.

Figura 23: Página de restauração de *backup*

6 CONSIDERAÇÕES FINAIS E RESULTADOS

Na rede sem fio fornecida pelo servidor ZeroShell, o tráfego de informações foi testado com até 12 máquinas, no evento *install fest* realizado na mostra tecnologia em 2009 no IFES campus Serra. As operações realizadas pelos alunos em suas máquinas neste evento geraram um tráfego considerável de dados, pois os alunos necessitavam baixar os pacotes para realizar a instalação de seus *softwares*. Os resultados de velocidade e desempenho foram satisfatórios, todos os alunos elogiaram a velocidade da conexão, e o desempenho da máquina.

O servidor ZeroShell mostrou-se apto a atender as necessidades dos polos, por ser de fácil instalação e configuração, não necessitar de máquina muito robusta para funcionar e por prover os serviços necessários para os laboratórios dos polos. Também é de baixo custo, pois utiliza softwares livres e gratuitos e não necessita de máquina muito robusta, com isso o custo de *hardware* também é baixo.

Entretanto não é recomendável que se utilize uma máquina com a configuração especificada no capitulo 5, ou uma máquina antiga para utilizá-la como o servidor da rede, pois pode ocorrer problemas freqüentemente, e caso alguma peça de *hardware* estrague sua reposição se torna inviável na maioria das vezes.

O servidor ZeroShell mostrou-se de muito fácil manutenção, caso ocorra problemas, a reinstalação é muito fácil e rápida. Com a possibilidade de restauração dos *backups* é possível restaurar as configurações que haviam antes da ocorrência do problema, com isso, a máquina volta a funcionar em curtíssimo espaço de tempo.

Por meio do mecanismo de *profiles* também é possível, que a configuração do ZeroShell seja realizada no CEAD e feito um *backup* do *profile* e enviado para os polos que restauram o *backup*, independente da arquitetura da máquina, e tudo funcionará corretamente. Com isso os polos não dependem de profissionais especializados na área para manter a rede do polo funcionando constantemente.

6.1 TRABALHOS FUTUROS

Com a evolução do CEAD, e o aumento da quantidade de cursos oferecidos, as necessidades de serviços dos polos podem aumentar, e a implementação dos serviços a seguir poderiam contribuir com a melhor qualidade de ensino:

- Balanceamento de carga;
- Autenticação com o Servidor RADIUS integrado com o LDAP e com o Captive Portal;
- Implementação da autenticação segura utilizando o Kerberos;
- Implementação de QoS;
- Implementação de VPN;

O balanceamento de carga é de grande importância quando um polo possui mais de um link de conexão com a internet, pois aumenta a utilização dos links não gerando sobrecarga em um link enquanto outro fica ocioso. Como o servidor ZeroShell tem suporte a conexão 3G é possível também fazer o balanceamento de carga entre um link adsl e a conexão 3G.

Com a autenticação do servidor RADIUS integrado com o LDAP e com o Captive Portal, a segurança da rede se torna maior, pois pessoas não autorizadas não podem acessar a rede.

A implementação da autenticação segura com o Kerberos é importante para evitar o roubo de informações, pois com o Kerberos os dados da autenticação são transmitidos criptografados.

Com a implementação do QoS é possível fazer a reserva de banda para determinados tráfegos de informações, com isso, pode-se garantir uma largura de banda para os serviços necessários para a EaD.

A implementação de VPN garante uma comunicação segura entre os pólos de apoio presencial e o CEAD. Com isso pode-se transmitir informações importantes pela VPN sem risco de interceptação dos dados.

7 REFERÊNCIAS BIBLIOGRÁFICAS

MELO, Sandro et al. **BS7799 da Tática à Prática em Servidores Linux**. 1. Ed. – Castelo Rio de Janeiro: AltaBooks, 2006.

KUROSE, James F. **Redes de Computadores e a internet: uma abordagem top-down** / James F. Kurose, Keith W Ross; Tradição Arlete Simille Marques; revisão técnica Wagner Luiz Zucchi. – 3. ed. – São Paulo : Pearson Addison Wesley, 2006.

MOURANI, Gerhard. ***Securing and Optimizing Linux: The Ultimate Solution***. 2. ed. – Canada: National library, 2001.

STREBE, Matthew e PERKINS, Charles. **Firewalls.** 1. ed. – São Paulo: MAKRON Books, 2002.

RICCIARD, Fulvio. **Router/Bridge Linux Firewall** Disponível em: http://www.zeroshell.net/eng/. Acesso em 07 dez. 2009.

TANENBAUM, Andrew S. Redes de Computadores / Andrew S. Tanenbaum; Tradução Vandenberg D. de Sousa. - 4. Ed. - Rio de janeiro: Elsevier, 2003.

LIMA, João Paulo de. **Administração de Redes Linux**. 1. Ed. – Goiânia: Terra, 2003.

CHIN, Liou Kuo. **Rede Privada Virtual - VPN**. Disponível em: http://www.rnp.br/newsgen/9811/vpn.html. Acesso em 10 dez. 2009.

DONALDSON, Bob, et al. – *Network Address Translation*. Disponível em: <http://searchenterprisewan.techtarget.com/sDefinition/0,,sid200_gci214107,00.html> Acesso em: 27 dez. 2009.

BATTISTI, Júlio. – Tutorial de TCP/IP – Parte 20 – NAT – *Network Address Translation*. Disponível em: < http://www.juliobattisti.com.br/artigos/windows/tcpip_p20.asp > Acesso em: 27 dez. 2009.

ALECRIM, Emerson. – Tecnologia Wi-Fi (IEEE 802.11). Disponível em: < http://www.infowester.com/wifi.php > Acesso em: 29 dez. 2009.

Wi-Fi Alliance. *Discover and Learn*. Disponível em < http://www.wi-fi.org/discover_and_learn.php> Acesso em 29 Dez. 2009.

UAB. Polo UAB. Disponível em <http://uab.capes.gov.br/index.php?option=com_content&view=article&id=103&Itemid=29> Acesso em 04 Jan. 2010a.

UAB. Exemplo de Polo EAD. Disponível em <http://mecsrv70.mec.gov.br/webuab/polo.php#> Acesso em 04 Jan. 2010b.

WIKIPEDIA. ***Wireless Distribution System***. Disponível em <http://pt.wikipedia.org/wiki/Wireless_Distribution_System> Acesso em 10 Fev. 2010.

INTERNET WORLD STATES. **INTERNET USAGE STATISTICS. The Internet Big Picture. World Internet Users and Population Stats**. Disponivel em <http://www.internetworldstats.com/stats.htm> acesso em 12 Fev. 2010.

HILGERS, Christian. ***HTTP Anti Virus Proxy: Documentation***. Disponível em <http://www.server-side.de/documentation.htm> acesso em 17 Fev. 2010.

BRADLEY, Tony. **Enable WEP or WPA Encryption To Protect Your Wireless Network: Scramble Your Data So That Others Can't Intercept It.** Disponivel em <http://netsecurity.about.com/od/quicktip1/qt/qtwifiwepwpa.htm> acesso em 17 Fev. 2010.

VIVASEMFIO. **Quebrar WPA**. Disponível em < http://www.vivasemfio.com/blog/category/wi_fi_protected_access_wpa/> Acesso em 17 Fev. 2010.

Instituto Federal de Educação, Ciência e Tecnologia do Espírito Santo – IFES

Modelo de Configuração de Servidor para os Polos de Educação a Distância com o uso de Software Livre

Curso: Redes de Computadores
Graduando: Everton Moschen Bada
Orientador: José Inácio Serafini

Contexto do Trabalho

- De acordo com o site *INTERNET WORLD STATES* a internet na América latina cresceu 890% em 2009.
- De acordo com o site do ABRAEAD, em 2007 a educação a distância cresceu 264%.
- O crescimento da Internet, o investimento público e as facilidades dessa modalidade de ensino estão impulsionando o crescimento da EaD via internet no Brasil.

Contexto do Trabalho

- De acordo com a UAB, entre 2007 e 2009 foram criados 557 polos de EaD, disponibilizando 187.154 vagas.

- O Centro de Educação a Distância do IFES, oferece cursos a distância do sistema UAB em parceria com prefeituras do estado do ES.

- Atualmente o CEAD possui parceria com 17 dos 26 polos existentes no ES.

Motivação

- A UAB define os requisitos de instalações, pessoal e equipamentos que um polo necessita.
- Entretanto a UAB não especifica a infraestrutura lógica da rede com serviços necessários para o polo.

Objetivos

- Propor um modelo de configuração de um servidor, incluindo as especificações mínimas de hardware, softwares e o sistema operacional para ser utilizado nos polos de EaD.

- O modelo de configuração proposto utilizará softwares livres, será de fácil instalação e configuração.

Pauta da Apresentação

- Metodologia;
- Serviços de Rede e Segurança;
- CEAD;
- Infraestrutura de um polo;
- Requisitos do servidor de um polo;
- Proposta do Trabalho;
- Estudo de caso com o ZeroShell;
- Resultados;
- Considerações finais;
- Dúvidas.

Metodologia

- Estudar e definir os serviços, tecnologias e protocolos necessários para os polos;
- Pesquisar tecnologias para suprir as necessidades dos polos;
- Estudar as tecnologias;
- Configurar as tecnologias, protocolos e serviços;
- Registrar o passo a passo da instalação e configuração do servidor.

Serviços de Rede e Segurança

- A solução proposta vai utilizar os seguintes serviços de rede:
  - Firewall;
  - Proxy;
  - DHCP;
  - NAT;
  - Wi-Fi.

Firewall

- O Firewall a ser utilizado será o *iptables*, por atuar em toda a pilha de protocolos, ser livre e ser bastante difundido no mercado.

Proxy

- O *proxy* a ser utilizado é o *HTTP Anti Virus Proxy* (HAVP) que possui as funcionalidades de um *proxy*, e verifica o tráfego de dados com antivírus, ClamAv.
- O antivírus ClamAv atualiza sua base de informações automaticamente. Ele também verifica imagens jpg, gif e png.

NAT

- NAT é um mecanismo que permite a tradução de um endereço IP utilizado dentro de uma rede para um diferente endereço IP conhecido em outra rede.
- O *software* a ser utilizado para fornecer esse mecanismo é o iptables.

Wi-Fi

- A solução provê o serviço de acesso sem fio (802.11) por meio de uma placa de rede instalada no servidor. Ela provê o serviço de um Access Point.

ZeroShell

- ZeroShell é uma distribuição Linux, que possui e integra vários serviços e protocolos.

- O ZeroShell foi desenvolvido por Fulvio Ricciard, administrador de sistemas do Instituto Nacional de Física Nuclear (INFN) – Itália em 2006.

- Atualmente encontra-se na versão 1.0 beta 12.

ZeroShell

- O ZeroShell funciona como *LiveCD,* entretanto ele pode ser instalado em unidades de armazenamento: HD, *pen drive* e *compact flash*.
- Para que as configurações do ZeroShell sejam salvas é utilizado um mecanismo conhecido como *profile*.

ZeroShell

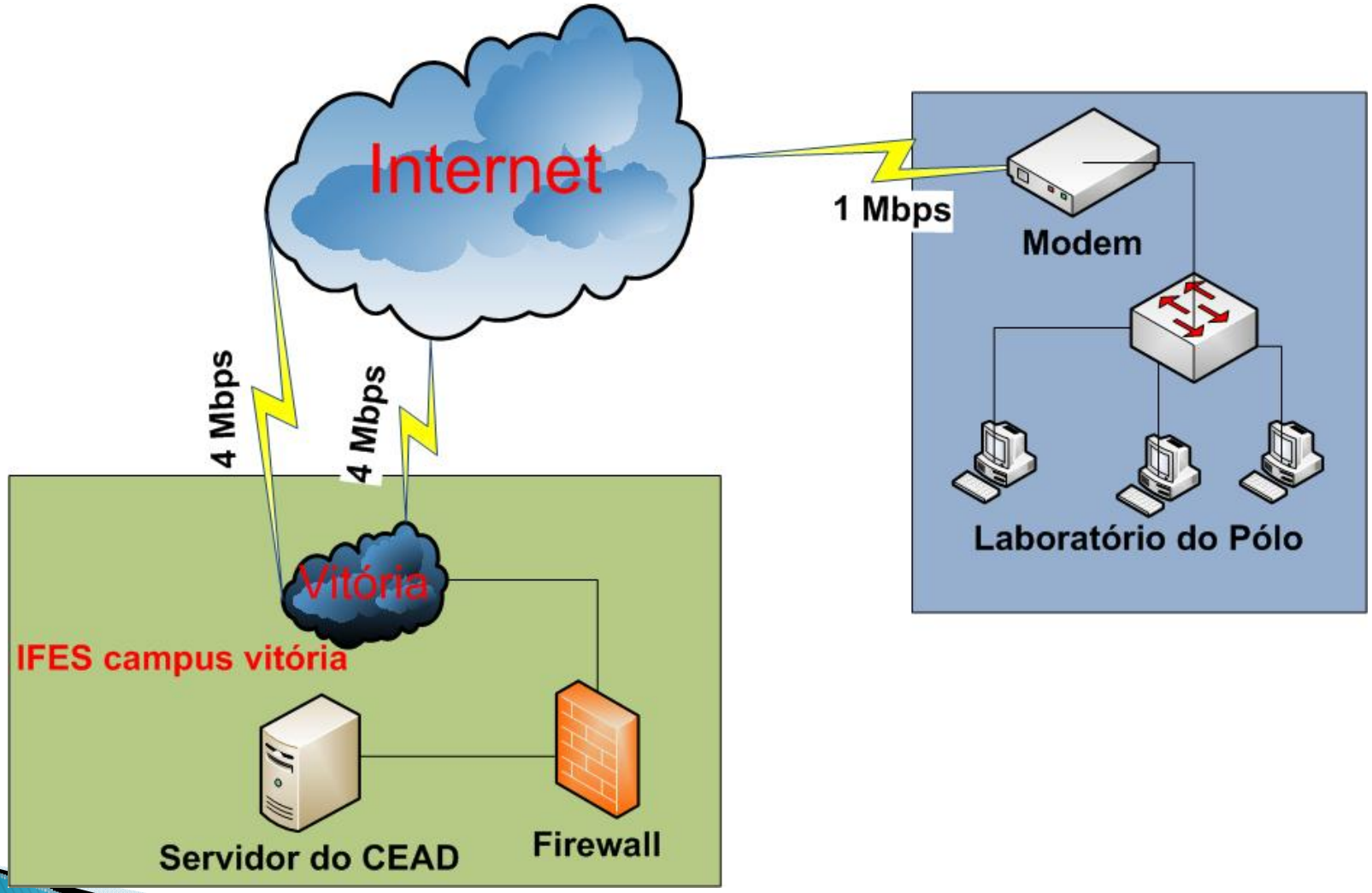
- O *profile* armazena as configurações e os Logs do sistema.

- O *profile* é independente da arquitetura do computador.

CEAD

- O CEAD, com sede no IFES campus Serra, é responsável pelos projetos de Educação a Distância (EaD) do IFES.
- Oferece cursos a distância do sistema da UAB, em parceria com as prefeituras pelo ES.
- Possui parceria 17 polos espalhados pelo ES.

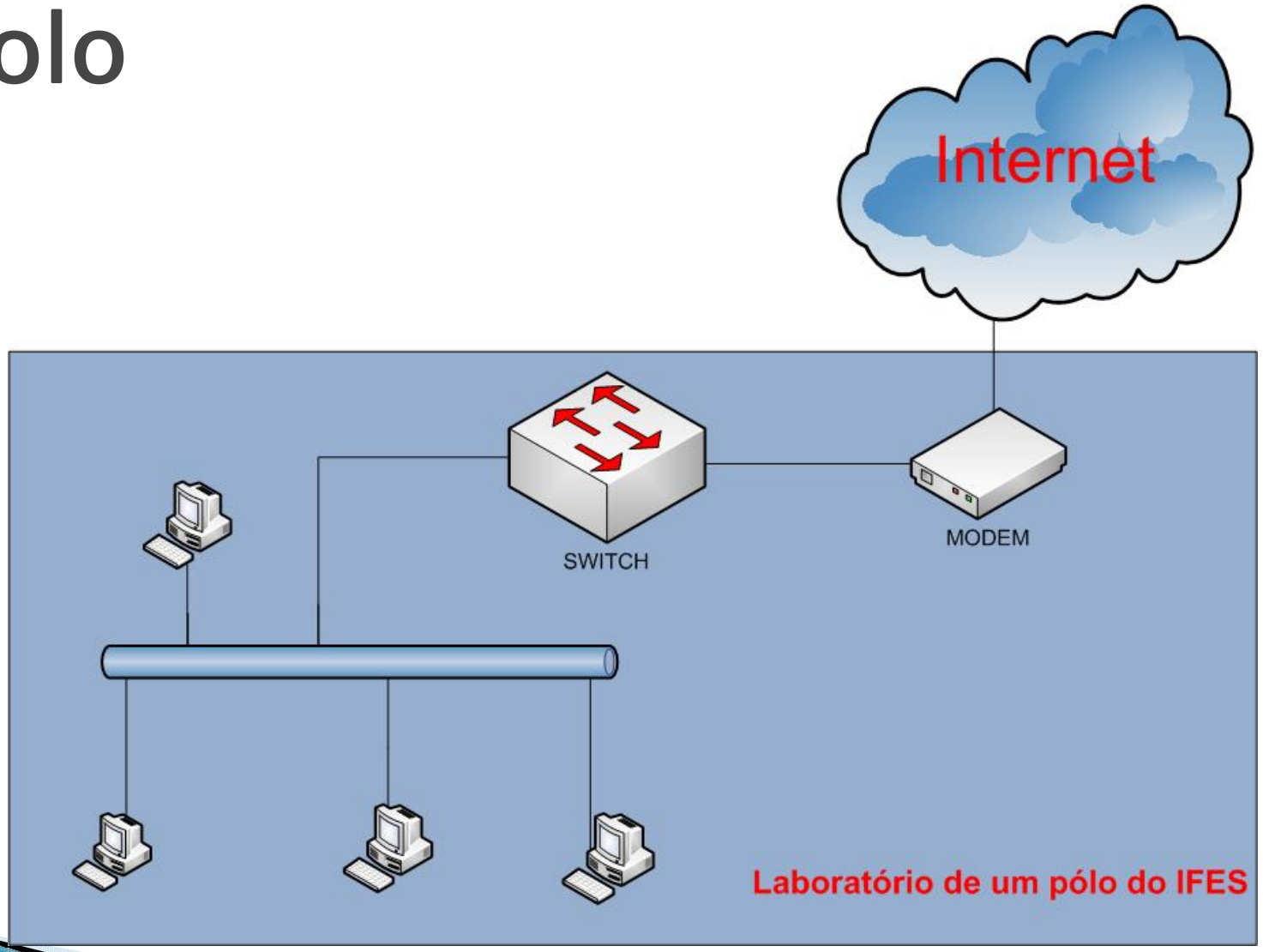
Infraestrutura de rede do CEAD



Polo de apoio presencial

- São espaços físicos mantidos por municípios ou governos de estado que oferecem infraestrutura física, tecnológica e pedagógica para que os alunos possam acompanhar os cursos da UAB.

Infraestrutura de rede de um polo



Polos da UAB no ES

Fonte: UAB

Requisitos do Servidor

- Para atender as necessidades dos polos o servidor necessita atender a requisitos de:
  - Segurança;
  - Desempenho;
  - *Backup.*

Requisitos de segurança

- Os requisitos de segurança são os seguintes:
  - Firewall;
  - Proxy;
  - Antivírus;
  - Autenticação para a rede sem-fio;
  - Verificar todas as páginas web e as imagens nos formatos jpg, gif e png com o antivírus;
  - Criar *Black List* de sites proibidos e *White List* para os sites permitidos.

Requisitos de desempenho

- Os requisitos de desempenho são os seguintes:
  - O servidor deve funcionar, em uma máquina com no mínimo de 256 MB de memória RAM, 20 GB de HD e processador Pentium 3.

Requisitos de *backup*

- Como requisito de *backup*, o programa deve realizar o *backup* das configurações e do Log do servidor.

- E que seja possível realizar o *backup* em horário que o polo não esteja em funcionamento.

Proposta de configuração

- Este trabalho propõe a utilização dos seguintes *softwares*, entre outros, para atender os requisitos de um servidor do polo:
  - iptables;
  - HAVP;
  - dhcpserver;
  - ZeroShell.

Um estudo de caso na aplicação da proposta

- Para validar a proposta, foi realizado um estudo de caso com a configuração do servidor e dos serviços, atendendo aos requisitos dos polos.

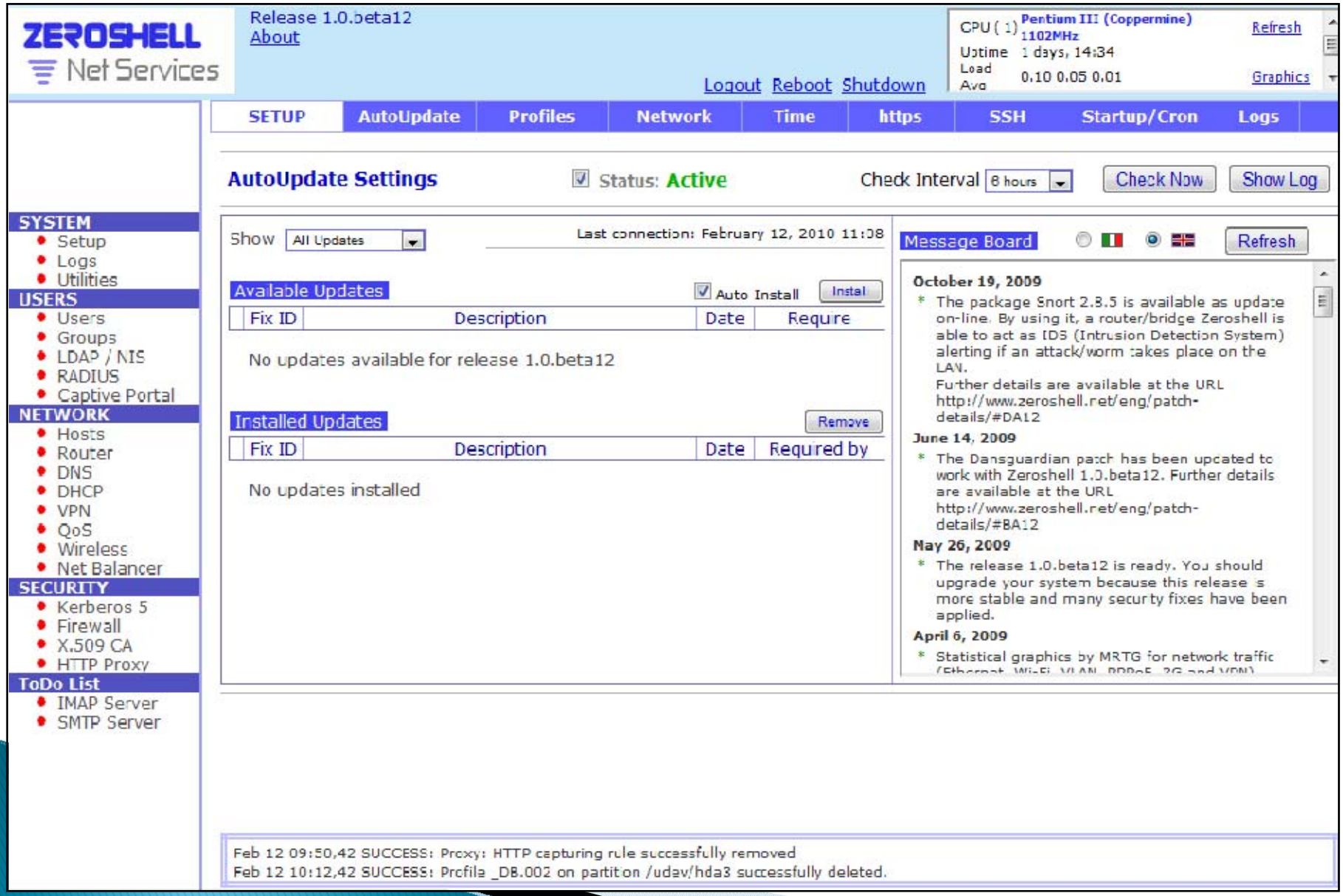
- Como o ZeroShell fornece todos os serviços, protocolos e tecnologias necessárias, de forma integrada, o processo torna-se relativamente rápido.

Um estudo de caso na aplicação da proposta

- O estudo de caso foi realizado em uma máquina com as configurações mínimas requeridas.

- A servidor ficou localizado no laboratório de TCC, disponibilizando alguns serviços.

ZeroShell– Interface Web



Resultados

- O ZeroShell foi testado no laboratório de TCC disponibilizando a rede sem-fio.
- Houve até 4 conexões simultâneas, todos os usuários elogiaram a velocidade da conexão e o desempenho do servidor.
- Os alunos que acompanharam a instalação e configuração ficaram impressionados com a facilidade de instalação e configuração dos serviços.

Considerações finais

- O ZeroShell mostrou-se apto a atender as necessidades dos polos, por possuir as seguintes características:
  - Fácil instalação;
  - Fácil configuração;
  - Facilidade de manutenção;
  - Baixo Custo de *hardware* e nenhum custo de *software*;
  - Fácil execução de *backup* e restauração de backup.

Dúvidas

Obrigado!!!

Graduando: Everton Moschen Bada
Orientador: José Inácio Serafini