UNIVERSIDADE FEDERAL DE SANTA MARIA
COLÉGIO TÉCNICO INDUSTRIAL DE SANTA MARIA
CURSO SUPERIOR DE TECNOLOGIA EM REDES DE COMPUTADORES

PROPOSTA DE REESTRUTURAÇÃO DA REDE LÓGICA DE ENDEREÇOS IPV4 DO HUSM COM ENFÂSE NA SEGURANÇA DE REDES

TRABALHO DE GRADUAÇÃO

Tiago Teixeira Portilho

Santa Maria, RS, Brasil

2014

PROPOSTA DE REESTRUTURAÇÃO DA REDE LÓGICA DE ENDEREÇOS IPV4 DO HUSM COM ENFÂSE NA SEGURANÇA DE REDES

Tiago Teixeira Portilho

Trabalho de Graduação apresentado ao Colégio Técnico Industrial da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para a obtenção do grau de

Tecnólogo em Redes de Computadores

Orientador: Prof. Me. Renato Preigschadt de Azevedo

Santa Maria, RS, Brasil

2014

Teixeira Portilho, Tiago

Proposta de Reestruturação da rede Lógica de endereços Ipv4 do HUSM com enfâse na Segurança de Redes / por Tiago Teixeira Portilho. – 2014.

36 f.: il.; 30 cm.

Orientador: Renato Preigschadt de Azevedo

Monografia (Graduação) - Universidade Federal de Santa Maria, Colégio Técnico Industrial de Santa Maria, Colégio Técnico Industrial, RS, 2014.

1. Redes de computadores. 2. Escalonamento. 3. Segurança. I. Azevedo, Renato Preigschadt de. II. Título.

E-mail: portilho@redes.ufsm.br

Universidade Federal de Santa Maria
Colégio Técnico Industrial de Santa Maria
Curso Superior de Tecnologia em redes de Computadores

A Comissão Examinadora, abaixo assinada,
aprova o Trabalho de Graduação

PROPOSTA DE REESTRUTURAÇÃO DA REDE LÓGICA DE ENDEREÇOS IPV4 DO HUSM COM ENFÂSE NA SEGURANÇA DE REDES

elaborado por
Tiago Teixeira Portilho

como requisito parcial para obtenção do grau de
Tecnólogo em Redes de Computadores

COMISSÃO EXAMINADORA:

Renato Preigschadt de Azevedo, Me.
(Presidente/Orientador)

Tiago Antonio Rizzetti, Me. (UFSM)

Thiago Cassio Krug, Bel. (UFSM)

Santa Maria, 11 de Dezembro de 2014.

AGRADECIMENTOS

Agradeço há todos meus familiares por me apoiarem em todos os momentos do curso.

Ao professor Renato Preigshadt de Azevedo, por me orientar no presente trabalho.

Ao professor Tiago Rizzetti, por me auxiliar em derterminados momentos.

Ao setor de informática do Hospital Universitário de Santa Maria, em especial ao Emerson Mortari e Fabiano Franco, pela confiança e incentivo durante o projeto.

RESUMO

Trabalho de Graduação
Curso Superior de Tecnologia em redes de Computadores
Universidade Federal de Santa Maria

PROPOSTA DE REESTRUTURAÇÃO DA REDE LÓGICA DE ENDEREÇOS IPV4 DO HUSM COM ENFÂSE NA SEGURANÇA DE REDES

AUTOR: TIAGO TEIXEIRA PORTILHO
ORIENTADOR: RENATO PREIGSCHADT DE AZEVEDO
Local da Defesa e Data: Santa Maria, 11 de Dezembro de 2014.

A utilização de aplicações web vem crescendo cada vez mais, tanto em instituições públicas, quanto em instituições privadas. Sendo assim o investimento em computadores e dispositivos de rede, tende a acompanhar esta crescente. Através deste acontecimento, ocasiona uma maior utilização de endereços IPv4(Internet Protocol version 4), e assuntos como facilidade de escalonamento e segurança, devem ser tratados pelos administradores de redes de computadores, com cuidado para evitar problemas. No HUSM(Hospital Universitário de Santa Maria), não é diferente, ou seja, também veem sofrendo uma crescente no número de computadores, afetando diretamente a utilização da rede. Devido a este fato, foi possível elaborar o presente trabalho, que aborda uma proposta de reestruturação da rede lógica de endereços IPv4*(Internet Protocol version 4)*, com ênfase na segurança. Em um primeiro momento, foram mapeadas as conectorizações entre os dispositivos de rede no hospital, logo após, foi feito um mapa da rede lógica, para analisar o tráfego existente na rede. Através deste foi possível verificar a existência de serviços como: *firewall, NAT(Network Address Transltion), VPN(Virtual Private Network)* e servidor de *proxy*, entre outros serviços internos. Também foi possível diagnosticar algumas fragilidades de segurança na rede lógica e dificuldade de escalonamento. Com base no diagnostico, a ideia é propor a segmentação da rede, a implementação de VLAN*(Virtual Local Area Network)*, novas configurações de servidor de *proxy*, implementação de *firewall* com alta disponibilidade e configurações nos *switches*, visando a segurança. O *pfsense* foi a ferramenta escolhida para proporcionar os serviços, em conjunto com o *Squid* e *SquidGuard*. Sendo assim foi possível elaborar um estudo de caso, para testar regras de *firewall*, configuração de VPN*(Virtual Private Network)* e *proxy*. Por fim este trabalho ressalta a importância de ter uma rede segmentada e suas configurações de segurança, como: *firewall, proxy*, entre outras. Devem ser configuradas cuidadosamente.

Palavras-chave: Redes de computadores. Escalonamento. Segurança.

ABSTRACT

Undergraduate Final Work
Graduate work Course of Technology in Computer networks Federal University of Santa Maria
Federal University of Santa Maria

PROPOSED RESTRUCTURING OF ADDRESS LOGIC NETWORK IPV4 THE UNIVERSITY HOSPITAL OF SANTA MARIA WITH THE EMPHASIS NETWORK SECURITY

AUTHOR: TIAGO TEIXEIRA PORTILHO
ADVISOR: RENATO PREIGSCHADT DE AZEVEDO
Defense Place and Date: Santa Maria, December 11st, 2014.

Not only in public institutions, but also in private institutions, the use of web applications has been increasing more and more. This way, the investment in computers and network devices tend to follow this increase. Through this, a bigger utilization of IPv4 (Internet Protocol version 4) addresses occurs and issues such as ease of scaling and security should be treated by the network administrators carefully to avoid problems. At the University Hospital of Santa Maria (HUSM), the problem is no different; in other words, it has also been suffering from a rising numbers of computers, directly affecting the network utilization. Due to this fact, the present study proposed to restructure the logical network of IPv4 addresses, with emphasis on security. Firstly, the connectorizations among the network devices of the hospital were mapped. After that, a map of the logical network was done to analyze the existing network traffic. It was possible to verify through this study the existence of services such as: firewall, Network Address Translation (NAT), Virtual Private Network (VPN) and proxy server, among other internal services. It was also possible to diagnose some security weaknesses on the logical network and scaling difficulty. Based on the diagnosis, the idea was to propose network segmentation, implementation of the Virtual Local Area Network (VLAN), new settings of the Proxy Server, implementation of firewall with high availability and configuration on the switches, aiming security. The pfsense was the tool chosen to provide the services, along with Squid and SquidGuard. Thus, it was possible to develop a case study to test firewall rules, VPN and Proxy configuration. Lastly, this study highlights the importance of having a segmented network with its security configurations, such as: firewall, Proxy, among others (which should be set carefully).

Keywords: Computer Networks. Scaling. Security.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

CPD	Centro de Processamento de Dados
DHCP	*Dynamic Host Configuration Protocol*
DNS	*Domain Name System*
AGHU	Aplicativo de Gestão para Hospitais Universitários
Sismama	Sistema de Informação do Câncer de Mama
Sie	Sistema de Informações para o Ensino
Sicel	Sistema de Controle de Exames Laboratoriais da Rede Nacional de Contagem Linfócitos
NAT	*Network Address Translation*
VPN	*Virtual private network*
HTTPS	*HyperText Transfer Protocol Secure*
ICMP	*Internet Control Message Protocol*
CARP	*Common Address Redundancy Protocol*
VRRP	*Virtual Router Redundancy Protocol*
IPV4	*Internet Protocol version 4*
HTTP	*HyperText Transfer Protocol*
HUSM	Hospital Universitário de Santa Maria
HTML	*HyperText Markup Language*
URL	*Uniform Resource Locator*
IP	*Internet Protocol*
STP	*spanning tree protocol*
UDP	*User Datagram Protocol*
TCP	*Transmission Control Protocol*

SUMÁRIO

INTRODUÇÃO

Para projetar uma rede endereçamentos IPv4*(Internet Protocol version 4)* é importante pensar na facilidade de escalonamento, para garantir que futuramente não falte endereços. A participação do responsável pela rede é fundamental, no qual pode informar o quanto a rede vai crescer em um futuro próximo, (OPPENHEIMER, 1999).

Quando acontece um broadcast em uma rede comutada, não é apenas o destinatário que visualiza os pacotes, e sim todos dispositivos conectados à rede. Como a tendência é que aumente o escalonamento da rede, então é visto que aumentará o broadcast na rede.Para evitar que um problema não se espalhe em toda a rede, segmentar a rede se torna uma obrigação para os administradores de rede. E este propósito pode ser feito através de VLAN (Virtual Local Area Network), o administrador da rede pode criar redes locais virtuais utilizando a mesma rede física e assim diminuir os problemas na rede, (KUROSE; ROSS, 2010).

Segurança de informações no campo da tecnologia da informação, vem crescendo constantemente, conforme a crescente usabilidade de aplicações web, com isso é interessante ter um controle de acesso, tanto do meio interno para o interno, interno para o externo, e externo para o interno, para tal tarefa existem tecnologias como *firewall, proxy e VPN (Virtual Private Network)*,(NAKAMURA; GEUS, 2007). Os dispositivos de redes como *switches* estão cada dia mais inteligentes, auxiliando em vários assuntos de rede de computadores, entre eles a segurança, com tecnologias como *port security e dhcp snooping*.

Todas essas funcionalidades de segurança, geralmente são instaladas em um único computador. Então caso ocorra uma falha no hardware deste computador, a rede pode ficar indisponível por um tempo. Para evitar este acontecimento, uma opção é a implementação de uma técnica de alta disponibilidade de *firewall*. Com isso a rede conta com no mínimo dois computadores dedicados para *firewall*, no qual um deles fica esperando o principal parar de funcionar, para assumir sua função.

O HUSM (Hospital Universitário de Santa Maria), está sofrendo uma crescente no número de equipamentos do seu parque tecnológico, no qual contribui com o aumento da utilização de endereços IPv4. Sendo assim o presente trabalho, apresenta uma proposta de reestruturação da rede lógica do HUSM, visando facilitar o escalonamento e aprimorar a segurança da rede lógica.

O escopo do trabalho limita-se, a planejar a segmentação da rede lógica de endereços

IPv4 e o emprego de *VLAN*. Além disso focar na segurança, elaborando um *firewall* com alta disponibilidade e política padrão adequada, propor uma configuração de *proxy* robusta e utilização de *VPN*. Também propor uma solução de configuração de *dhcp snooping e port security*.

O trabalho segue a seguinte organização: no Capítulo 2 aborda alguns assuntos relacionados, para facilitar a compreensão. O Capítulo 3 apresenta um diagnostico da rede atual e a proposta de reestruturação. O Capítulo 4 apresenta o estudo de caso com base na proposta. O Capítulo 5 apresenta as conclusões finais e a proposta de trabalhos futuros.

2 CONCEITOS RELACIONADOS

2.1 Endereçamento IP versão 4

Para que um computador funcione na *internet* ele deve ter um endereço IP *(Internet Protocol)*. O IP é constituído por 32 *bits*, sendo que, uma parte corresponde como identificador de início e final da rede, e outra por *hosts* usuais. Os endereços de rede são utilizados pelos roteadores para fazer rotas entre redes. Inicialmente foram criadas faixais de endereços privados e globais, para evitar conflitos entre empresas, sendo que, privados só se comunicam com a rede interna da empresa e globais são roteados em toda a *internet* (SOUSA, 2013).

Para endereços Ipv4 privados terem acesso a toda rede internet, foi criado a tecnologia NAT *(Network Address Translation)*. A tecnologia requer que ao menos um computador na rede *internet*, tenha um endereço IPv4 privado e global, geralmente esse computador é o roteador da rede interna. Após configurado o NAT *(Network Address Translation)* no roteador, ele traduz o endereço Ipv4 privado, do computador que tentou comunicação com um endereço IPv4 global, para o seu próprio, endereço Ipv4 global.

2.2 Switchs

Switches são equipamentos inteligentes que definem um domínio de colisão para cada interface, diferentes de *hubs* que possuem um domínio de colisão para todas *interfaces*. Sendo assim o *switch* consegue estabelecer um *link* ponto a ponto com duas máquinas, após a primeira comunicação entre elas, e enviar os *frames* diretamente uma para outra, um dos motivos que isso é possível é a existência da tabela de *mac address* em cada *switch* (FILIPETTI, 2008).

Alguns *switches* também tratam questões de segurança na rede, dois destes recursos são o *dhcp snooping* e *port security*. O primeiro recurso trata de prevenir que, um usuário mal intencionado ou até mesmo por não ter conhecimento, habilite um servidor DHCP *(Dynamic Host Configuration Protocol)* em seu *desktop* ou *laptop*, e cause um grave problema de segmentação na rede. Este serviço segue a premissa de *interfaces* confiáveis ou não confiáveis, sendo que as portas confiáveis são os servidores DHCP da rede e as *interfaces up-links*, que são as interfaces que interligam os *switches* (CISCO, 2012).

Atualmente é bem comum projetistas de rede elaborarem uma forma de redundância entre *switches*, para garantir disponibilidade da rede. Porém para evitar que aconteça uma dupli-

cação de *frames* e formação de *loops* na rede é fundamental adotar uma técnica para detcção de *loops*, para tal tarefa existe o protocolo STP *(Spanning Tree Protocol)*. Os *switches* comunicam-se através de BPDU *(Bridge Protocol Data Unit)* para estabelecer quem será o *switch-root*, este *switch* será responsavél por gerenciar toda rede. A escolha do *switch-root* é feita através de um cálculo do BID (valor de identificação do *switch*, padrão 32768) + *mac address* de cada *switch*, ou seja, o *switch* que estiver o menor valor é eleito o *switch root*, e os outros switches serão nomeados como não *root*. O *switch root* habilita suas *interfaces* para receber e enviar *frames*, nos *switchs* não *root* é feito um cálculo de menor custo até chegar ao *switch root*. Para saber qual *interface* será habilitada como porta designada, ou seja, por onde enviará e receberá *frames*, e a *interface* que terá o maior custo será bloqueada para evitar o *looping* (SOUSA, 2013).

2.3 VLAN

VLAN *(Virtual Local Area Network)*, reduz o domínios de *broadcast*, permite um agrupamento lógico de usuários e possibilitam uma melhora no gerenciamento da rede local. Atuante na camada de *enlace* VLAN não se comunicam com VLAN. Sendo assim é aconselhável definir uma rede IP para cada VLAN, no qual a comunicação entre VLAN acontece na camada de rede. existem dois tipos de configuração de VLAN estática e dinâmica, o primeiro modo a configuração é feita manualmente, ou seja, o administrador da rede entra no *switch* e configura a VLAN, o segundo acontece através de um VMPS *(VLAN Management Policy Server)* e um banco de dados com os endereços físicos da rede (FILIPETTI, 2008).

2.3.1 Interface Trunk e Access

Para diferenciar as *VLAN*, os *switches* utilizam as *tags* que cada *VLAN* tem. Essa *tag* é inclusa no *frame ethernet*. As *interfaces trunk* são configuradas para encaminhar as *tags*, para os demais *switches* da rede, por um mesmo *link* físico, o protocolo predominante para este serviço é o 802.q. As *interfaces access* ou *untagged* já recebem o *frame* sem a *tag*, ou seja, prontas para a utilização de computadores finais (KUROSE; ROSS, 2010).

2.4 Firewall

Nas organizações os usuários dependem cada vez mais da *internet* para realizar suas tarefas, com isso a preocupação com a segurança tende a crescer. Em consequência pode-se notar

uma rápida evolução nessa área, principalmente em relação ao *firewall*. O *firewall* é constituído por diversas funcionalidades que exercem diferentes funções, isso interfere diretamente na segurança do sistema. Existem funcionalidades clássicas como: (filtros, *proxies*, *bastion hosts*, zona desmilitarizada). Também foram inseridas funcionalidades como: VPN *(Virtual Private Network)* e *proxy server* (NAKAMURA; GEUS, 2007).

O *proxy* é um filtro que atua na camada de aplicação, sendo capaz de atuar de forma transparente ou não transparente. O modo transparente ele fica escutando o que passa pela rede, na qual bloqueia o que é nescessário, sendo que neste modo ele não bloqueia as conexões HTTPS *(HyperText Transfer Protocol Secure)*. O modo não transparente ele trabalha de modo interativo com o usuário, pois todas as conexões são iniciadas do servidor de *proxy*, sendo assim consegue bloquear conexões HTTPS (CHESWICK, 2005).

A aplicação que mais tem destaque no mundo é a WWW *(World Wide Web)*, através dela os usuários tem acesso as páginas *web*, que são elaboradas na maioria das vezes com uma linguagem de marcação de hipertexto HTML. Essas páginas disponibilizam, documentos de textos, imagens, videos entre outros. Todo esse conteúdo fica armazenado em um servidor *Web*, normalmente o *Apache*, que é acessado via *browser* exemplo: *Chrome, Firefox, Internet Explorer*. O *browser* faz uma requisição utilizando a URL da página, por meio do protocolo HTTP, ao servidor *web* onde esta armazenada o conteúdo da página (KUROSE; ROSS, 2010).

Cada aplicação *web* detém um endereço IP para ser acessado na rede *internet*, que na maioria das vezes esse endereço é alterado, o mesmo acontece em ambientes com vários computadores, que são gerenciados por um pequeno grupo de pessoas. Seria inviável para os usuários acessar inúmeras páginas *web* apenas pelo seu IP ou o setor de informática lembrar dos IPs de inúmeros servidores, com certeza para a maioria dos seres humanos lembrar um nome do que uma sequência de números é mais fácil. Para solucionar este problema foi criado o DNS *(Domain Name System)*, este sistema consiste de uma arquitetura cliente-servidor que atua de forma hierárquica com o intuito de resolver nomes para endereços IPs e também endereços Ips para nomes. Basicamento existe uma aplicação que o cliente faz uma consulta ao servidor que trata de traduzir os nomes para endereços IPs e vice-versa. Todo esse procedimento utiliza o protocolo de transporte UDP na porta 53 (TANEBAUM; WETHERALL, 2011).

3 LEVANTAMENTO DA REDE ATUAL E PROJETO DE REESTRUTURAÇÃO

3.1 Rede Atual

3.1.1 Estrutura Física da Rede

No hospital Universitário de Santa Maria – RS existe um parque tecnológico com: *desktops*, servidores, impressoras, aprelhos de videoconferências, câmeras, equipamentos hospitalares e *switches*. O prédio principal possui um subsolo e seis andares, fora isso encontra-se anexos que neste trabalho será tratado como extensão do subsolo. Do segundo ao sexto andar existe um *switch* por andar, e o restante dos *switches* estão distribuídos pelo primeiro andar e o subsolo. A Figura 3.1 ilustra como está a conexão da infraestrutura física da rede atualmente, onde os principais pontos são a sala de informática e o data center, localizados no primeiro andar. Na sala de informática existem dois *switches*, no qual um possui uma conexão de fibra ótica com o CPD (Centro de Processamento de Dados), e uma conexão via par trançado com o *firewall*. O outro *switch*, está conectado via par trançado com o *firewall* e os demais *switches*, no qual um deles encaminha para o *data center*. Onde estão todos computadores servidores, como o DHCP *(Dynamic Host Configuration Protocol)* e o AGHU (Aplicativo de Gestão para Hospitais Universitários). Nota-se que a Figura 3.1 não ilustra nenhuma representação de impressoras, ou *desktops*, entre outros, porém é válido lembrar que estes dispositivos estão todos conectados nos *switches* representados na Figura 3.1.

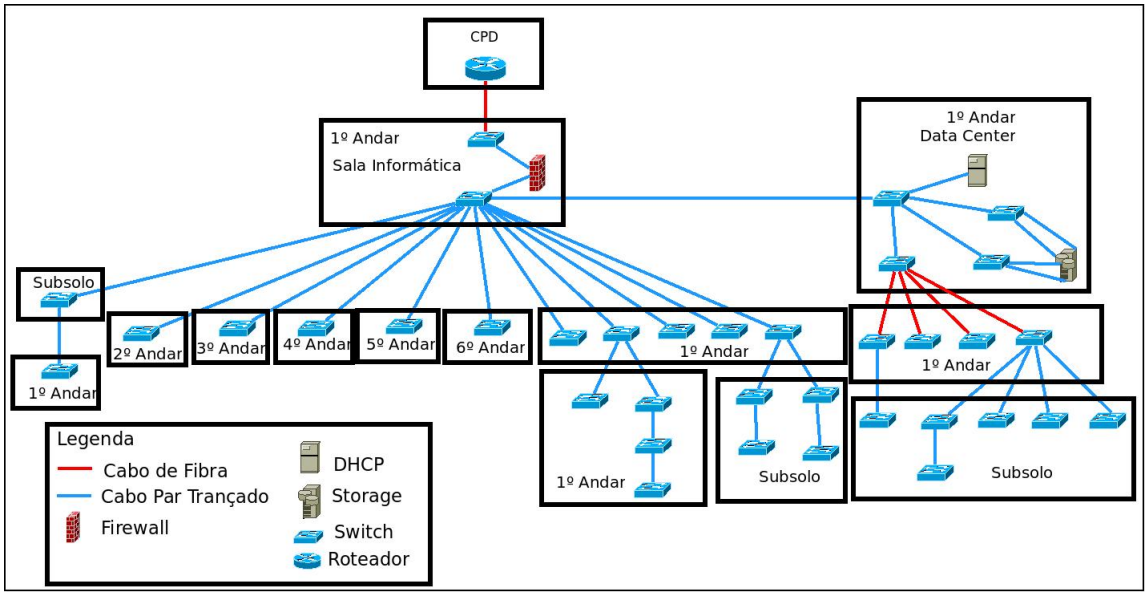


Figura 3.1 – Topologia Física da Rede

Está sendo executado um projeto que vai alterar a interconexão entre os *switches*. A figura 3.2 representa esta alteração, onde o cabo de fibra ótica que interliga o CPD com o HUSM, vai ser conectado em um *switch* do *data center*. A partir de um outro *switch* dentro do *data center*, será interconectado com os demais *switches* de todos os andares via fibra ótica. Sendo que haverá, redundância em alguns pontos do hospital, como, por exemplo: do 3º andar para o 4º andar.

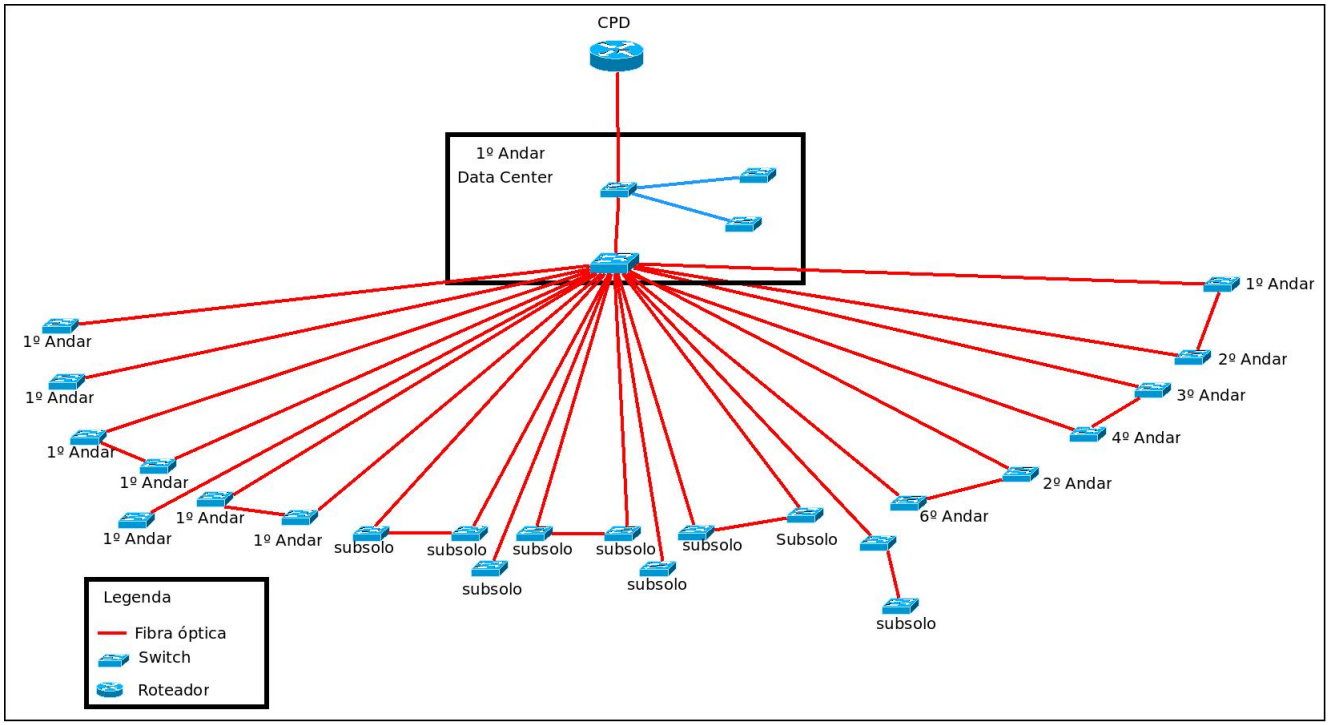


Figura 3.2 – Topologia Física da Rede após as mudanças físicas

3.1.2 Estrutura Lógica da Rede

A rede lógica é subdividida em três redes, uma rede com endereços IPv4 globais e outras duas redes com endereços IPv4 privados. Sendo que a 192.168.15.0/24 apenas para gerência de *switches* e câmeras, e a 192.168.192.0/22 para *desktops*, impressoras e servidores. Os *gateways* das redes estão no CPD (Centro de Processamento de Dados), da UFSM (Universidade Federal de Santa Maria). As rotas das redes são todas feitas no CPD e as configurações que exitem nos *switches*, são apenas de endereços IPv4 da rede 192.168.15.0/24, para gerência, ou seja, não existe outra configuração, à não ser por *default*.

Há uma série de aplicações que envolvem a rede, tanto do meio interno quanto no externo. As principais aplicações internas são: DHCP *(Dynamic Host Configuration Protocol)*, DNS *(Domain Name System)*, impressão, AGHU (Aplicativo de Gestão para Hospitais Universitários), Sismama (Sistema de Informação do Câncer de Mama), Anti-vírus, Redmine(Sistema de Gerência de projetos), Sie (Sistema de Informações para o Ensino), *Openldap* (Sistema de autenticação de usuários), *Active Directory*, *cacti* (Gerênciador de Ativos na Rede), site do hospital. Para cada aplicação existe no mínimo um servidor no *data center*.

A Figura 3.3 ilustra que todos os acessos, tanto do meio interno para o externo, quanto

do meio externo para o interno, passam pelo *firewall* da rede, que atua como *bridge*. O *firewall* utilizado é o *iptables*, com uma política padrão, *accept*, ou seja, aceita todos os pacotes, além disso está instalado o *proxy squid* de modo transparente ao usuário. O acesso ao meio externo está representado pelas setas roxas, que se resume a, atualizações de sistemas como o *Wsus* (Servidor de Atualizações do *Windows*), sites de pesquisa, videoconferências, e o Sicel (Sistema de Controle de Exames Laboratoriais da Rede Nacional de Contagem Linfócitos), que são feitos via NAT *(Network Address Translation)*. As setas pretas indicam o acesso para os *gateways* das redes.

O acesso externo para o meio interno é necessário, devido a administração dos servidores remotamente e certas exceções. Alguns servidores são administrados por terceiros, no qual, utilizam VPN IPsec e VPN PPTP, para estabelecer uma conexão, representados com as setas vermelhas e azuis respectivamente na Figura 3.3. Sendo que a PPTP também é utilizada pelos funcionários do setor de informática, representados pelas setas amarelas. As exceções são, departamentos do campus que precisam executar aplicações, em que os servidores estão instalados no hospital, no qual o acesso é feito via redirecionamento de porta, indicados pelas setas verdes.

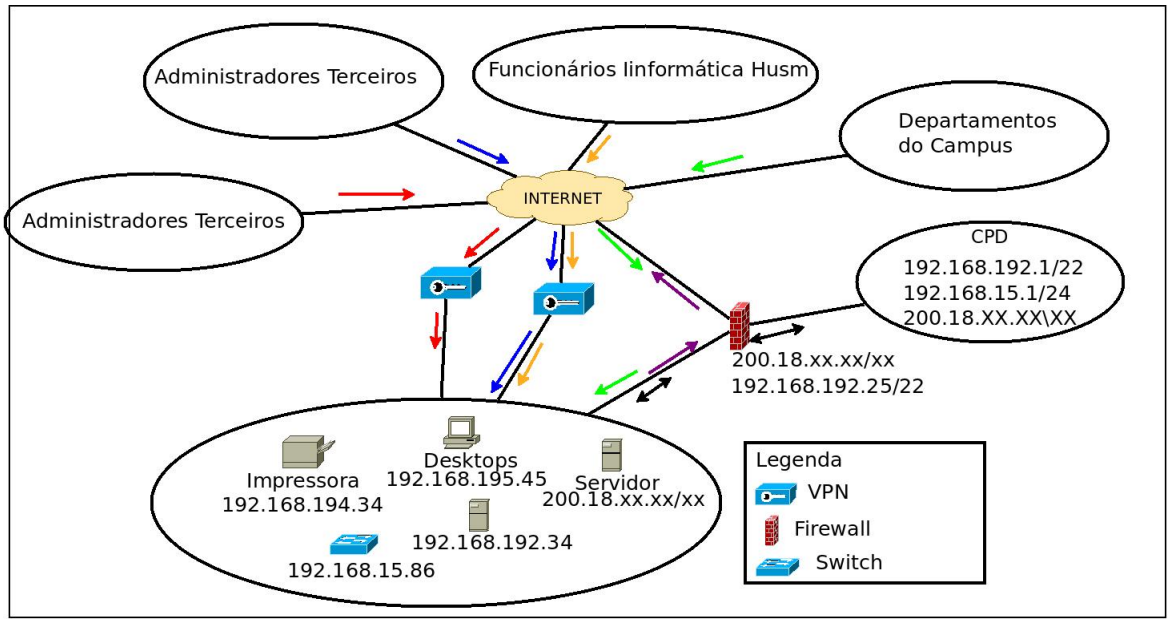


Figura 3.3 – Topologia Lógica da Rede

3.2 Proposta

Após diálogos com alguns funcionários do setor de informática do hospital, e a análise do tráfego da rede lógica. Foi possível diagnosticar problemas na rede, nos quais são: falta de endereços IPv4 privados, devido as redes serem criadas no CPD, inundação de *broadcast* na rede, fragilidade no *firewall*, fragilidade no *proxy*, excesso de liberdade para as *VPN*. Baseado nos problemas citados, e na infraestrutura física existente que virá a existir, tornou-se possível elaborar um projeto de reestruturação da rede lógica, visando facilitar o escalonamento e a segurança da rede.

3.2.1 Pfsense

Existem sistemas operacionais *open source* editados para desempenhar funções de gerência e segurança de rede, com o propósito de facilitar a tarefa dos administradores de rede. O *pfsense* é uma dessas ferramentas, iniciado por colaboradores do projeto *m0n0wall*, foi baseado no freebsd, com todas suas funcionalidades gerenciáveis via *web*. Além de atuar como *firewall*, disponibiliza serviços como roteamento, VPN, alta disponibilidade de *firewall*, entre outros. Também é possível instalar pacotes direcionados a redes de computadores como: *squid, squidguard*.

O *pfsense* herdou o PF *(Packet Filter)* do *freeBSD*, e segue umas caracteristicas padrões, ou seja, atua como *stateful* com uma política padrão *Drop*, na qual descarta todos os pacotes. Além disso ao configurar uma rede ele faz o roteamento desta rede com as redes existentes. Sendo assim não é preciso fazer rotas para as redes se comunicarem, apenas liberar regras de *firewall*.

Por ser um sistema robusto e ter uma *interface* de gerência amigável foi proposto a utilização do *pfsense* para disponibilizar os serviços, de segmentação da rede, roteamento, *firewall* e alta disponibilidade de *firewall*.

3.2.1.1 Segmentação da Rede

Para minimizar a falta de endereços IPv4 e inundação de *broadcast*, será proposto a segmentação da rede e criação de VLAN para cada rede. As VLAN foram elaboradas visando a segurança da rede lógica, sendo assim, criou-se uma VLAN somente para acessar as aplicações internas e algumas exceções externas, chamada *intranet*, e outra para acessar aplicações

externas e ou internas, chamada *internet*. Pensando em diminuir a inundação de *broadcast* e melhorar o escalonamento, será criado uma VLAN *intranet* e *internet*, com redes de prefixo /22, independente para cada andar. Com prerrogativa do primeiro andar, onde existem alguns setores que requerem VLAN separadas, como o *data center* e a sala de informática. No *data center* os servidores que precisam ser acessado por terceiros ficarão na VLAN *ServerItranet2*, os demais servidores ficarão na *ServerIntranet*. O setor de informática ficará na VLAN informática. Outros casos independentes são: Vlan equipamentos-hops, para equipamentos hospitalares, VLAN dispositivos para câmeras, e a VLAN gerência, para *switches*. A tabela 3.1 ilustra as configurações das VLAN e das subredes.

Tabela 3.1 – VLANS

Andar	**Vlan Nome**	**Vlan ID**	**Rede**
1º	ServerIntranet	1001	172.17.0.0/22
1º	ServerIntranet2	1005	172.17.4.0/22
1º	Informatica	1003	172.17.8.0/22
1º	Impressoras	1004	172.17.12.0/22
1º	Equipamento Hosp	1002	172.17.16.0/22
1º 2º 3º 4º 5º 6º Subsolo	Gerencia	1006	172.17.20.0/22
1º 2º 3º 4º 5º 6º	Dispositivos	1007	172.17.24.0/22
1º	Intranet1	1000	172.17.28.0/22
1º	Internet1	11	172.17.32.0/22
1º 2º	Intranet2	2	172.17.36.0/22
1º 2º	Internet2	12	172.17.40.0/22
1º 3º	Intranet3	3	172.17.44.0/22
1º 3º	Internet3	13	172.17.48.0/22
1º 4º	Intranet4	4	172.17.52.0/22
1º 4º	Internet4	14	172.17.56.0/22
1º 5º	Intranet5	5	172.17.60.0/22
1º 5º	Internet5	15	172.17.64.0/22
1º 6º	Intranet6	6	172.17.68.0/22
1º 6º	Internet6	16	172.17.72.0/22
1º Subsolo	IntranetSubSolo	7	172.17.76.0/22
1º Subsolo	InternetSubSolo	17	172.17.80.0/22

3.2.1.2 Firewall

Feita a segmentação da rede é possível elaborar uma arquitetura de *firewall*, para diminuir a fragilidade de segurança da rede lógica. O primeiro objetivo é a filtragem do tráfego interno, ou seja, o que cada subrede precisa acessar em outra. As subredes dos *desktops*, que são as *intranet* e as *internet*, precisam acessar as aplicações que ficarão nas subredes *ServerIn-*

tranet, *ServerIntranet2* e Impressoras. Para a subrede impressoras será liberado apenas a porta 9100, responsável por impressões. A subrede *ServerIntranet* terá acesso livre para qualquer destino, diferente da subrede *ServerIntranet2* que terá acesso apenas a algumas aplicações da *ServerIntranet*. A subrede informática terá acesso liberado para todas as subredes. A tabela 3.2 mostra as configurações de regras que serão criadas. É válido lembrar que a política padrão do *firewall* é *drop*, ou seja, descartar todos os pacotes.

Tabela 3.2 – Acesso Interno

Protocolo	**Origem**	**Destino**	**Porta**	**Aplicação**
TCP/UDP	Intranets e Internets	ServerIntranet	*	*
TCP/UDP	Intranets e Internets	ServerIntranet2	*	*
TCP/UDP	Intranets e Internets	Impressoras	9100 * Impressão	
ICMP	Intranets e Internets	*	*	
TCP/UDP	ServerIntranet	*	*	*
ICMP	ServerIntranet	*	*	*
TCP/UDP	ServerIntranet2	ServerIntranet	389	Ldap
TCP	ServerIntranet2	ServerIntranet	13782	Netbackup
TCP	ServerIntranet2	ServerIntranet	13783	Netbackup
TCP	ServerIntranet2	ServerIntranet	13720	Netbackup
TCP	ServerIntranet2	ServerIntranet	13724	Netbackup
TCP	ServerIntranet2	ServerIntranet	1556	Netbackup
TCP	ServerIntranet2	ServerIntranet	2821	Netbackup
TCP	ServerIntranet2	ServerIntranet	4032	Netbackup
ICMP	ServerIntranet2	*	*	*
TCP/UDP	informatica	172.17.0.0/16	*	*
ICMP	informatica	*	*	*
TCP/UDP	gerencia	gerencia	*	*
TCP/UDP	gerencia	ServerIntranet	*	*
ICMP	gerencia	*	*	*
TCP/UDP	dispositivos	dispositivos	*	*
ICMP	dispositivos	*	*	*
UDP	impressoras	*	123	*
ICMP	impressoras	*	*	*

O acesso interno para o meio externo será permitido, apenas para as subredes que precisam se comunicar com o meio externo, as quais são: as subredes *intranet, internet, ServerIntranet, ServerIntranet2,* informática. Para possibilitar este acesso será feito *nat outbound*, além de filtrar por regras de *firewall*. Também será proposto a utilização de *proxy* não transparente e não autenticado, para as subredes *intranet*, *internet* e informática.

Como na tabela 3.2 indica que será liberado todas as conexões originadas da rede *ServerIntranet*, então basta liberar as conexões que não são feitas via *proxy*. A tabela 3.3 ilustra

que será liberado todas as conexões originadas da rede *ServerIntranet2* para qualquer destino do meio externo, diferente das subredes *intranet, internet* e informática, será liberado conexões destinadas para o Sie e Sicel.

Tabela 3.3 – Tabela de acesso Externo

Protocolo	**Origem**	**Destino**	**Porta**	**Aplicação**
TCP/UDP	ServerIntranet2	*	*	*
TCP/UDP	intranets e internets	*	*	Sie
TCP/UDP	informatica	*	*	Sie

O *proxy* utilizado será o *squid* em conjunto com o *squidguard*, o *squid* é um serviço de *proxy* para *web*, ele trabalha de forma transparente ou não transparente, também faz *cache* de arquivos para economizar banda. O *squidguard* é uma extensão *squid*, ou seja, quando o *squid* recebe uma conexão ele direciona para o *squidguard* que filtra a URL, no qual disponibiliza uma *blacklist* para auxiliar a configuração de filtragem. Também é possível criar grupos de acesso por usuários, *ranges* de IP, subredes entre outros.

Será proposto a criação de grupos por subredes, ou seja, grupo da informática, *intranet* e *internet*. Sendo que a *intranet* terá tudo bloqueado por *default* e só serão liberados *sites* no campus e algumas exceções, listados na tabela 3.4, na qual indica o nome do arquivo, o assunto que ele trata e um exemplo de *site* que existe dentro do arquivo.

Tabela 3.4 – Grupo Intranets

Arquivo	**Assunto**	**Exemplo**
blk-BL-hospitals	hospitais	www.santacasa.org.br
blk-BL-universidades	universidades	www.ufsm.br

A informática e *internet* terão tudo liberado por padrão e será bloqueados alguns sites, listados na tabela 3.5, com os mesmos itens da tabela 3.4.

Tabela 3.5 – Informática e Internets

Arquivo	**Assunto**	**Exemplo**
blk-BL-adv	Banner	*
blk-BL-anonvpn	Sites acesso via VPN	*
blk-BL-chat	Bate-papo	www.terra.com.br
blk-BL-costtraps	*	www.cash4downloads.com
blk-BL-dating	relacionamento	almas.terra.com.br
blk-BL-gamble	jogos	zodiaccasino.com
blk-BL-hacking	*	mafia-linkz.to

O acesso do meio externo para o meio interno, continuará sendo por VPN e redirecionamento de porta via NAT, porém com certas mudanças representadas na Figura 3.4. A VPN IPSec utilizada por administradores terceiros será mantida, porém os usuários só terão acesso à subrede *ServerIntranet2*, representados pelas setas roxas. Outros administradores terceiros utilizarão *OpenVPN* para acessar suas aplicações na rede *ServerIntranet2*, representados pelas setas azuis. Os funcionários do setor de informática do hospital, utilizarão uma outra *OpenVPN*, e terão acesso a todas subredes, representado pelas setas vermelhas. O acesso dos departamentos do campus continuará sendo por redirecionamento de porta via NAT, sendo que, só terão acesso a subrede *ServerIntranet2*, representados com as setas verdes.

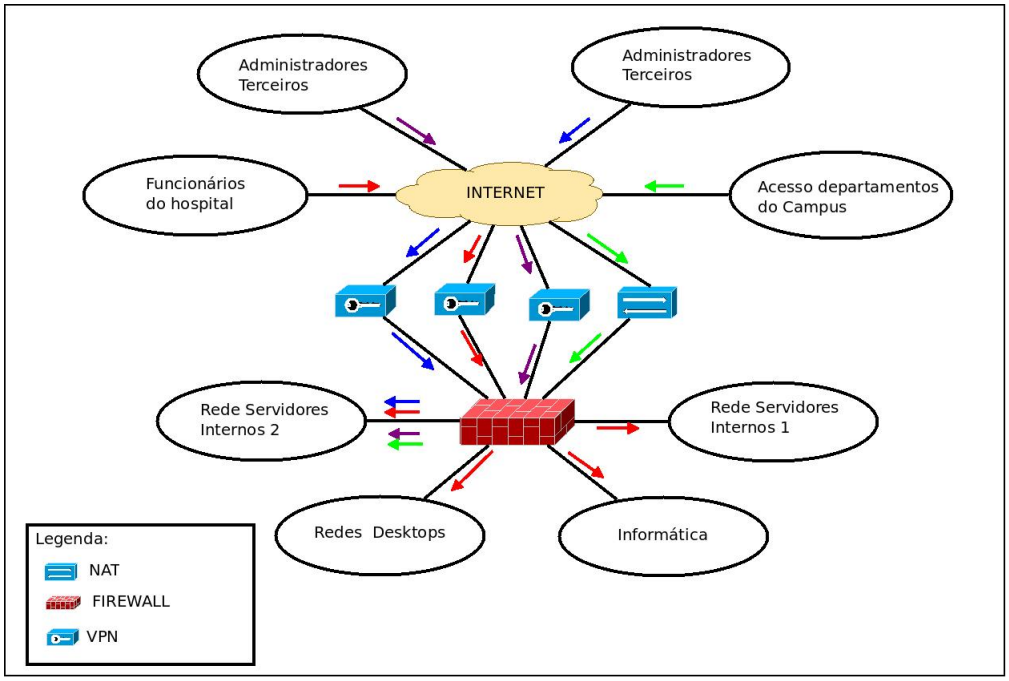


Figura 3.4 – Nova Topologia Lógica da Rede

OpenVPN é uma opção de VPN *(Network Private Virtual)* que proporciona uma segurança maior de criptografia, do que a PPTP. Sendo assim podemos escolher as redes no qual será feito o roteamento. Então as redes que tiverem rotas poderão ser acessadas.

3.2.1.3 Redundância de Firewall

O *pfsense* desfruta do protocolo CARP *(Common Address Redundancy Protocol)* nativo do *freeBSD*, para disponibilizar redundância de *firewall*, o qual surgiu como uma alternativa para o VRRP *(Virtual Router Redundancy Protocol)*. Através do CARP é possível criar um *cluster* de *firewall* onde um deles atua como *master* e o restante como *backups*. Ele utiliza da

técnica de IP virtual, em que para cada subrede existe um IP virtual, o qual serão os *gateways* das subredes. Os IP virtuais ficam alocados ao *firewall master*, que tem a maior prioridade, uma vez que o *master* fica *down* o IP virtual flutua para o próximo *backup* que tiver maior prioridade.

A partir da interface *pfsync* é possível manter a sincronização entre os *firewalls* e manter as regras de *firewall* atualizadas nas duas máquinas, ou seja, ao criar uma regra em uma máquina ele repassa para as seguintes.

Para adquirir alta disponibilidade de *firewall* vão ser configurados dois computadores, sendo assim serão utilizados três *interfaces* físicas para cada um, a *interface* wan com endereço IP público, a interface *lan*, na qual serão configuradas as VLAN com endereços IP privados e outra conectando os dois com endereço IP privado, conforme ilustra a Figura 3.5.

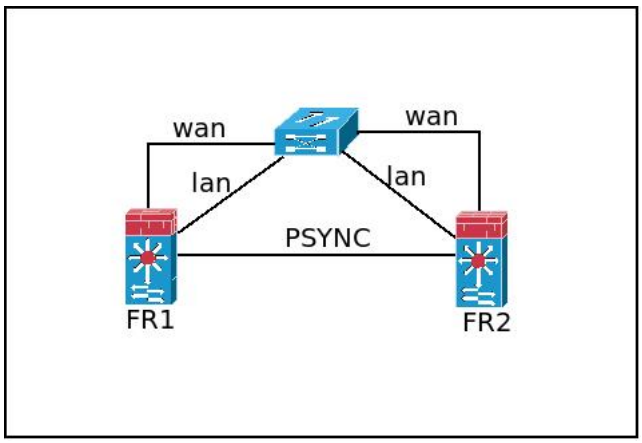


Figura 3.5 – Redunância de *Firewall*

A tabela 3.6 ilustra a distribuição dos endereços IP para os firewalls, no qual o Pfsense1 e o Pfsense2, terão um IP global, um IP de cada subrede e um IP da subrede do pfsync. Os IP Virtuais serão os gateways das subredes.

Tabela 3.6 – Endereçamento das Sub-redes

Interface	**Pfsense1**	**Pfsense2**	**IP Virtual**
wan	200.18.XX.XX	200.18.XX.XX	X
ServerIntranet	172.17.0.2/22	172.17.0.3/22	172.17.0.1/22
ServerIntranet2	172.17.4.2/22	172.17.4.3/22	172.17.4.1/22
Informatica	172.17.8.2/22	172.17.8.3/22	172.17.8.1/22
Impressoras	172.17.12.2/22	172.17.12.3/22	172.17.12.1/22
Equipamentos Hosp	172.17.16.2/22	172.17.16.3/22	172.17.16.1/22
Gerencia	172.17.20.2/22	172.17.20.3/22	172.17.20.1/22
Dispositivos	172.17.24.2/22	172.17.24.3/22	172.17.24.1/22
Intranet1	172.17.28.2/22	172.17.28.3/22	172.17.28.1/22
Internet1	172.17.32.2/22	172.17.32.3/22	172.17.32.1/22
Intranet2	172.17.36.2/22	172.17.36.3/22	172.17.36.1/22
Internet2	172.17.40.2/22	172.17.40.3/22	172.17.40.1/22
Intranet3	172.17.44.2/22	172.17.44.1/22	172.17.44.1/22
Internet3	172.17.48.2/22	172.17.48.3/22	172.17.48.1/22
Intranet4	172.17.52.2/22	172.17.52.3/22	172.17.52.1/22
Internet4	172.17.56.2/22	172.17.56.3/22	172.17.56.1/22
Intranet5	172.17.60.2/22	172.17.60.3/22	172.17.60.1/22
Internet5	172.17.64.2/22	172.17.64.3/22	172.17.64.1/22
Intranet6	172.17.68.2/22	172.17.68.3/22	172.17.68.1/22
Internet6	172.17.72.2/22	172.17.72.3/22	172.17.72.1/22
IntranetSubsolo	172.17.76.2/22	172.17.76.3/22	172.17.76.1/22
InternetSubsolo	172.17.80.2/22	172.17.80.3/22	172.17.80.1/22
pfsync	10.1.1.1/24	10.1.1.2/24	X

3.2.1.4 Switch

Baseado na Figura 3.2 será proposto a configuração do STP *(spanning tree protocol)*. Onde o *switch root* será o que tem conexão com os demais, sendo assim o *Bridge priority* deve ser configurado com um valor pequeno para garantir que ele seja o *root*. Nos demais basta habilitar o STP que as configurações necessárias vão acontecer automaticamente. Além disso também será habilitado o serviço *port security*, em todas as interfaces que são utilizadas por *desktops*, de todas VLAN *intranet* e *internet*. Também será configurado o DHCP *snooping*, no qual, as portas confiáveis serão todas as portas *uplinks* e a *interface* onde está conectado o servidor DHCP.

As configurações de VLAN nos *switches* serão baseadas nas localizações de cada *switch*, ou seja, só serão configuradas as VLAN que precisão trafegar em cada *switch*. Sendo que as VLAN gerência e impressoras, estarão em todos os *switches*. No *switch root* será configurado as *tag* de todas *VLAN*, no setor de informática será configurado, a informática, no segundo andar,

a *intranet1 intranet2*, *internet1* e *internet2*. No terceiro andar, a *intranet3*, *intranet4*, *internet3* e *internet4*, no quarto a *intranet3*, *intranet4*, *internet3* e *internet4*, no quinto a *intranet5*, *internet5*, *intranet6* e *intranet6*, no subsolo, a *intranetsubsolo*, *intranet1*, *internet2* e *internetsubosolo*. As *interfaces untagged*, depende do está conectado em cada *inteface*, e as *interfaces* trunk serão todas as *uplinks*.

4 ESTUDO DE CASO

Para o estudo de caso foram utilizados dois computadores físicos, no qual foi instalado o *pfsense* versão 2.1.5 em cada um, também foi utilizado um *switch* HP. A Figura 4.1 ilustra uma parte da tela inicial do *pfsense* com algumas configurações de *interfaces wan*, *lan* e algumas subredes, tais como a informática, também é possível visualizar o processador, a versão do sistema operacional e o *hostname* da máquina.

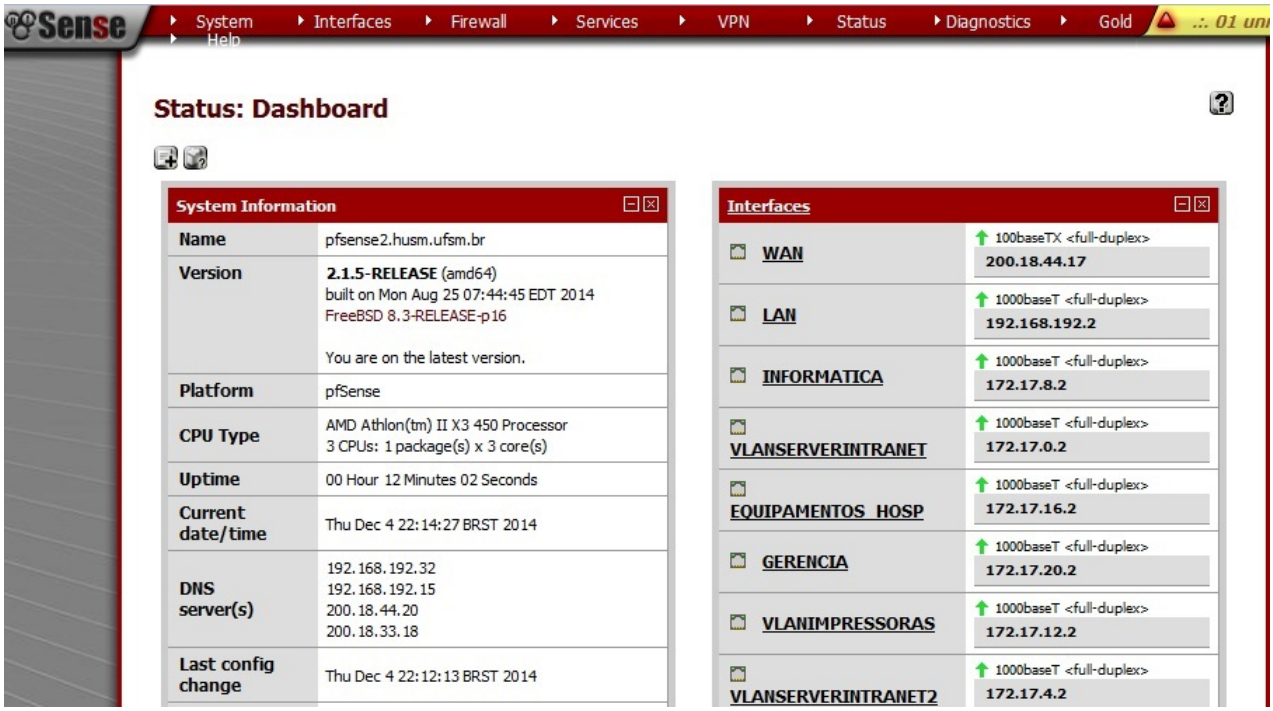


Figura 4.1 – *Pfsense.*

Para satisfazer as tabelas 3.2 e 3.3 foram implementadas as regras de *firewall* nas *interfaces* das suberedes. A Figura 4.2 ilustra a configuração das regras na *interface intranet1*, no qual indica qual protocolo de transporte está sendo utilizado, qual rede e porta de origem, e rede e porta de destino.

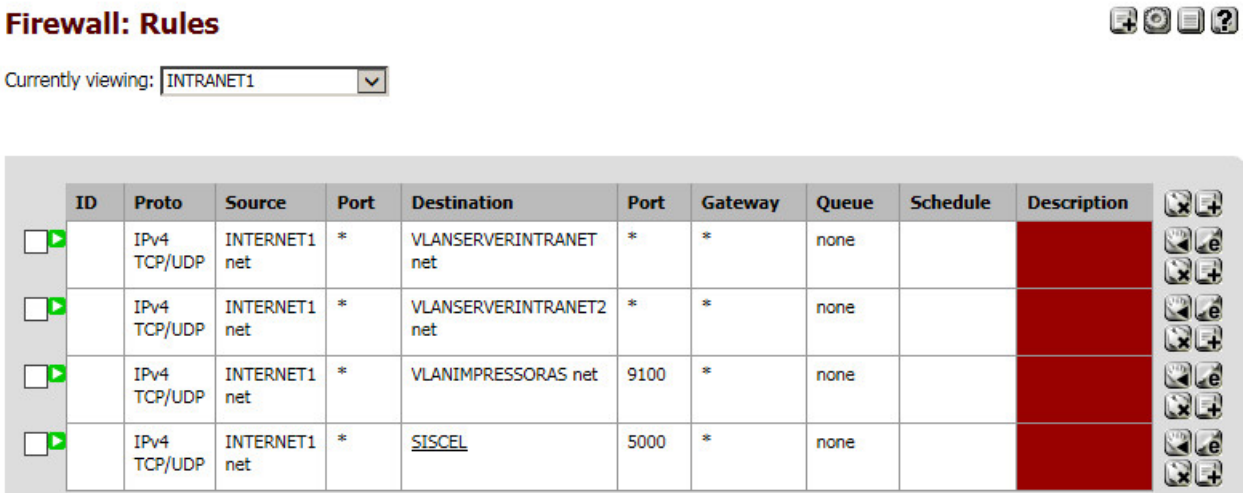
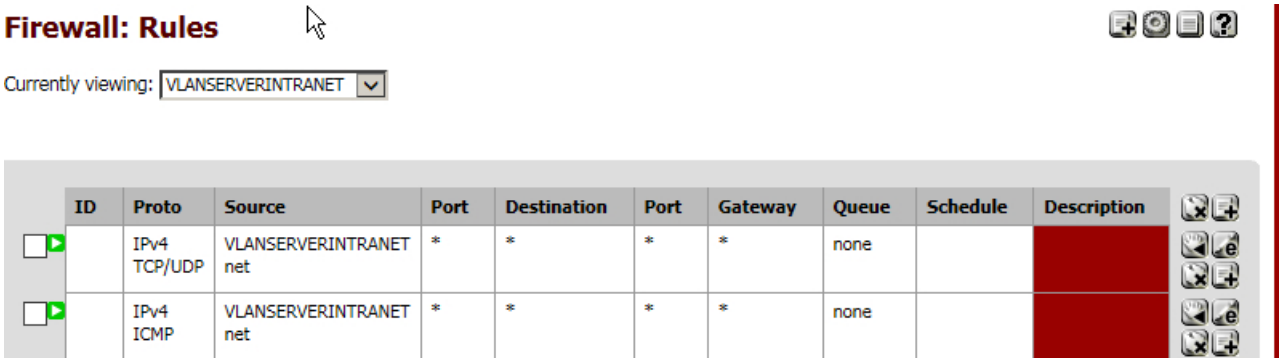
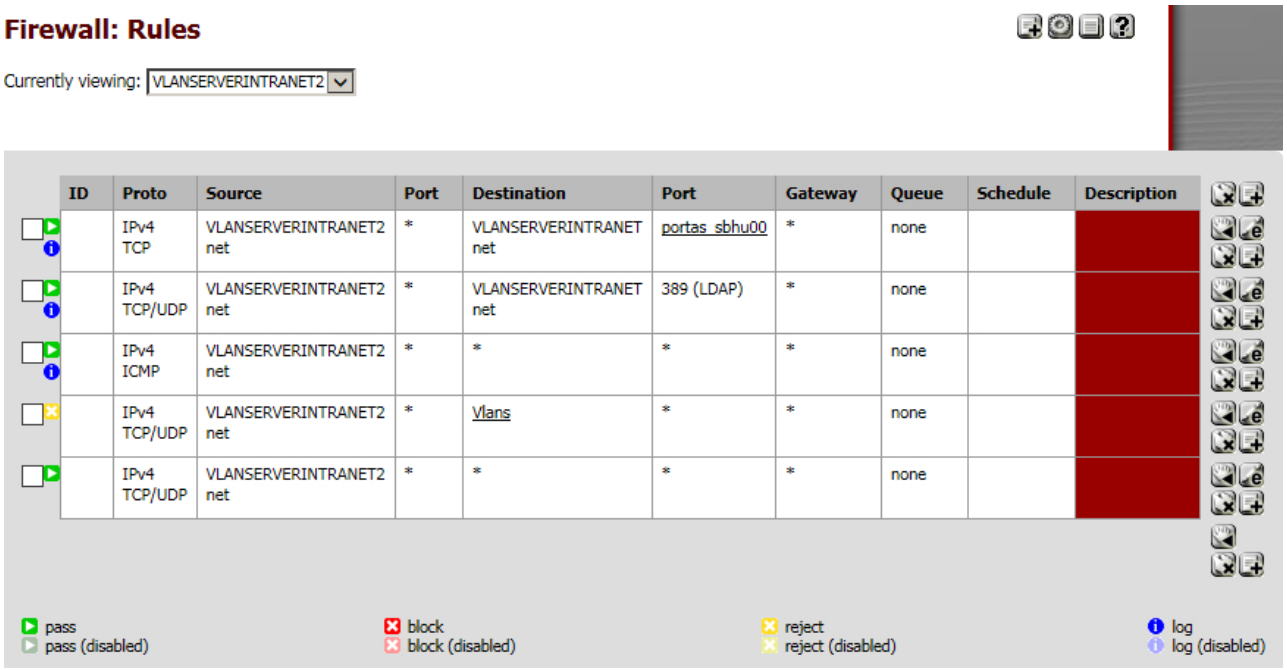


Figura 4.2 – Regras *Intranet1*.

A Figura 4.3 ilustra as configurações das subredes *ServerIntranet* e *Serverintranet2*, respectivamente, em que a primeira tem acesso liberado para qualquer destino via protocolo de transporte TCP, UDP e ICMP. A segunda inicia com a regra liberando acesso para subrede *ServerIntranet* nas portas sbhu00, o qual é um alias referente a portas do *netbackup*, a regra seguinte libera acesso para a mesma subrede na porta referente ao protocolo LDAP(*Lightweight Directory Access Protocol*), cuja sua função é autenticar usuários.



(a) Primeira



(b) Segunda

Figura 4.3 – Regras ServerIntranet e ServerIntranet2.

A Figura 4.4 ilustra a configuração do *squid*, no qual as opção utilizadas foram:

- *Proxy interface: interface* na qual os clientes vão mandar a solicitação;
- *Allow users on interface:* indica que todas as *interface* passaram pelo *proxy*;
- *Enable logging:* habilita os *logs do squid*;
- *Log store directory:* local dos *logs do squid*;
- *Proxy port:* Porta que o *squid* vai escutar;
- *Suppress Squid Version:* Não exibe a versão do *squid*;

- *Custom Options:* Insere opção no arquivo de configurações do *squid*, no qual foram inseridos o *http port* 172.17.0.1:3128, e *redirect program* redirecionamento para o *squidguard*.

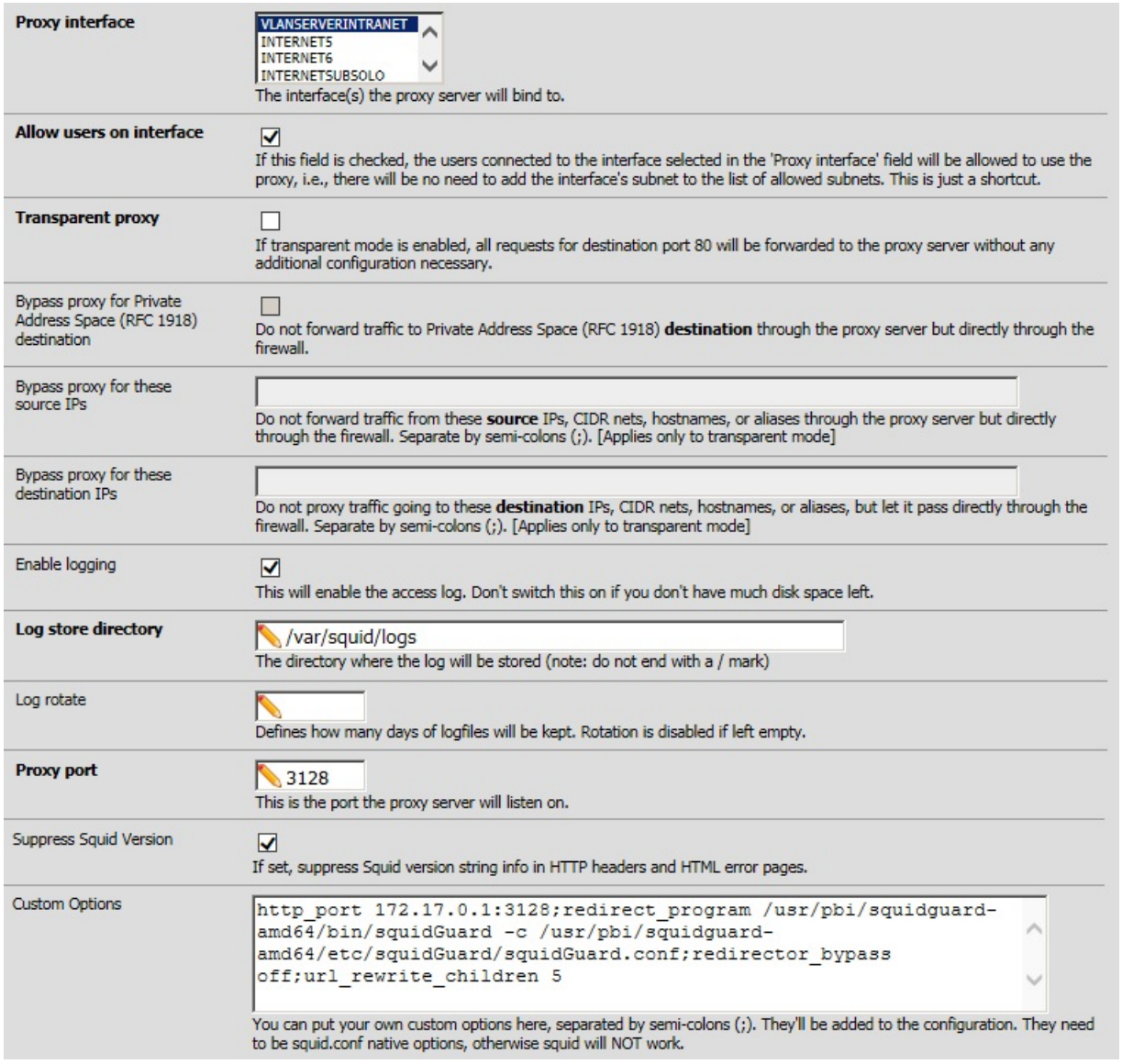


Figura 4.4 – Configuração do *Squid.*

A Figura 4.5 ilusta uma lista de endereços criada no *squidguard*, para ser liberados em todos os grupos de acesso. Sendo que no *Name* refere-se ao no da lista e o *Domain list* indica os dominios e endereços que contém a lista.

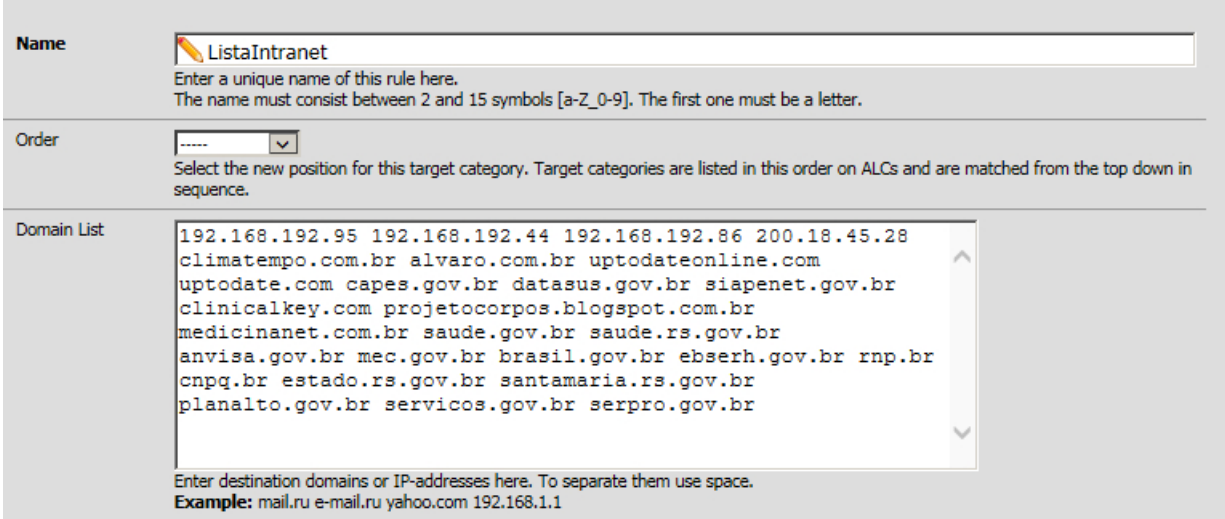


Figura 4.5 – *Lista Endereços.*

A Figura 4.6 ilustra o grupo de acesso *intranet*, onde vale ressaltar as principais configurações:

- *Name:* nome do grupo;
- *Client source:* clientes que fazem parte do grupo, no qual são todas as redes *intranet*;
- *Target rules list:* a lista de regras dos assuntos que vão ser permitidos neste grupo, no qual são apenas a Lista*Intranet* criada anteriormente, e por *default* tudo bloqueado.

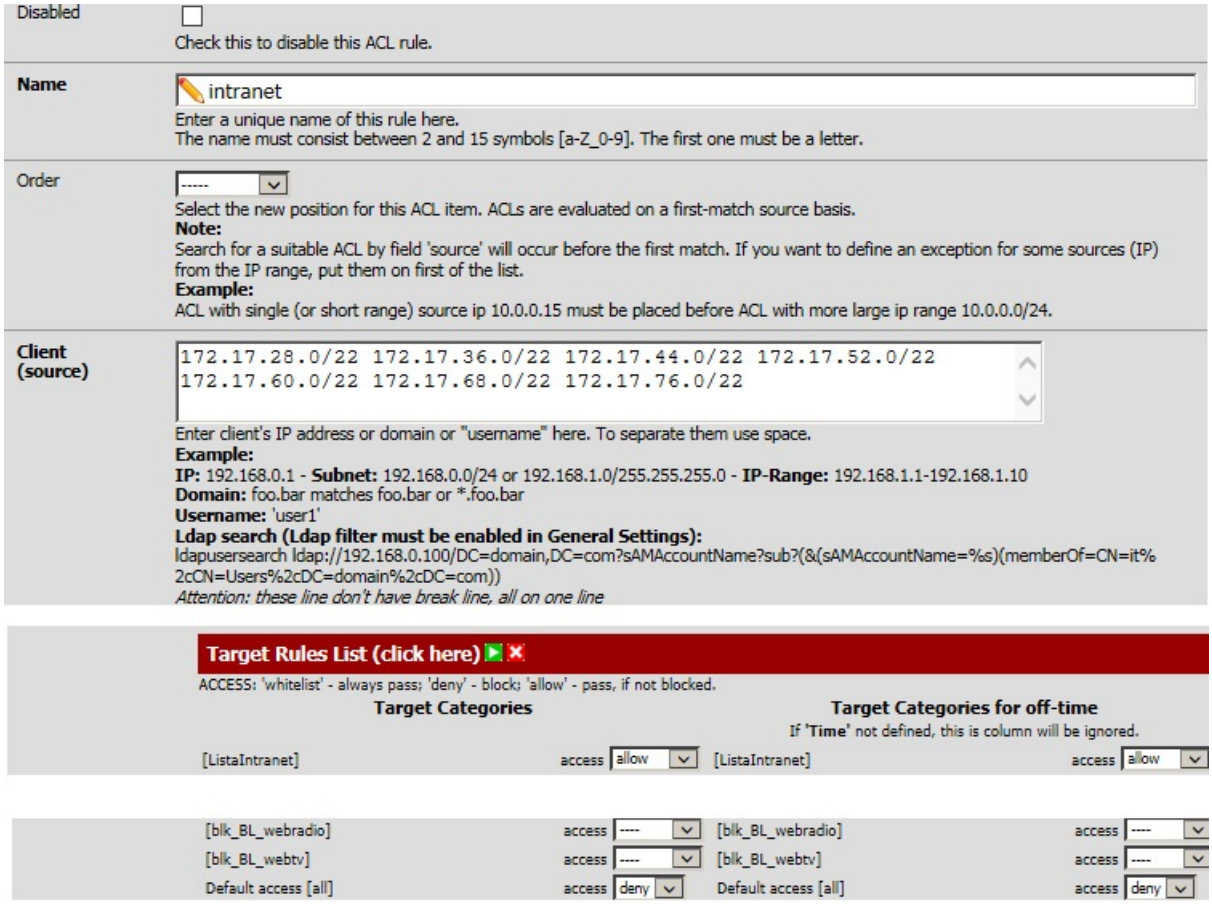


Figura 4.6 – *Lista Endereços.*

A Figura 4.7 mostra a tela com as *OpenVPN* criadas, sendo que a primeira está configurada para receber requisições na porta 1194 com o protocolo de transporte UDP, e estabelece o túnel com endereços IPv4 da rede 10.10.10.0/24. A segunda opção indica a configuração de segunda *OpenVPN*, porém utilizando a porta 31128 e rede para o túnel 192.168.0.0/24. Em seguida indica a configuração do túnel 10.10.10.0/24 e a rede na qual a mesma vai ser roteada, no qual é a 172.17.0.0/22.

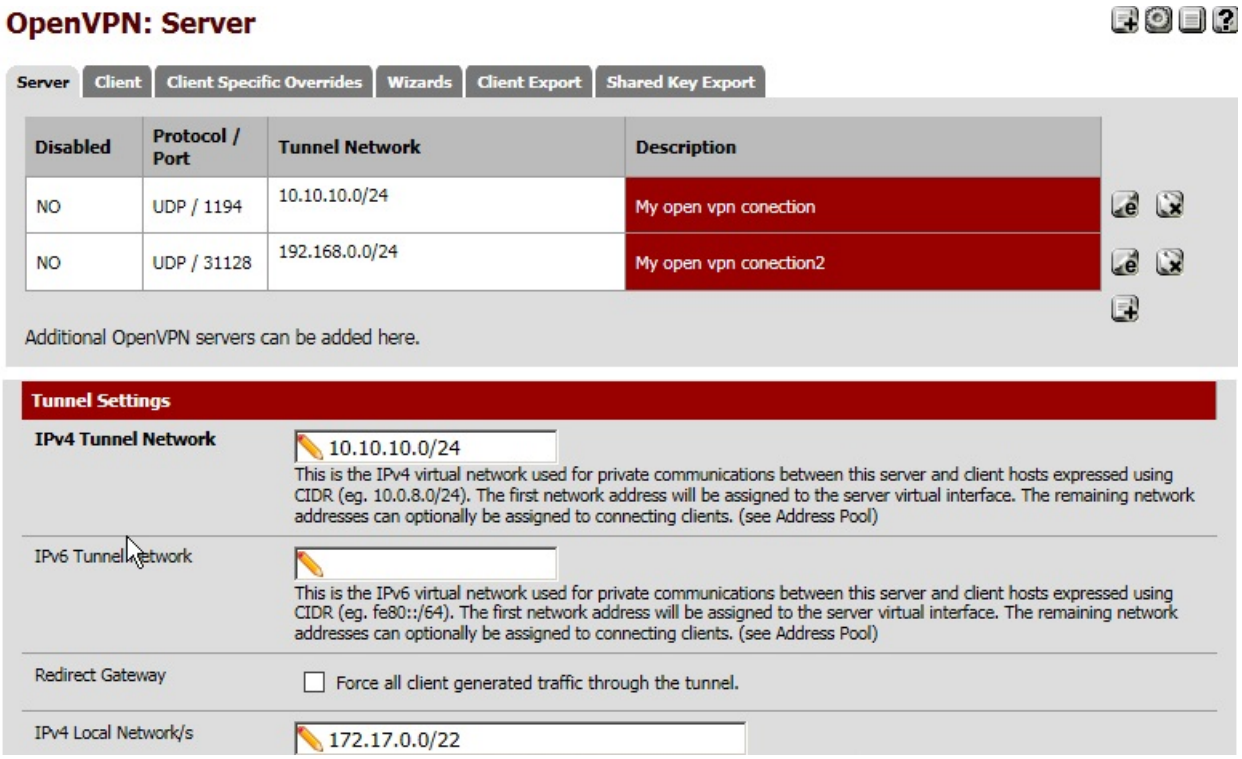


Figura 4.7 – *OpenVPN.*

A Figura 4.8 ilustra a comunicação da *interface pfsync* mantendo a sincronia entre os *firewalls*

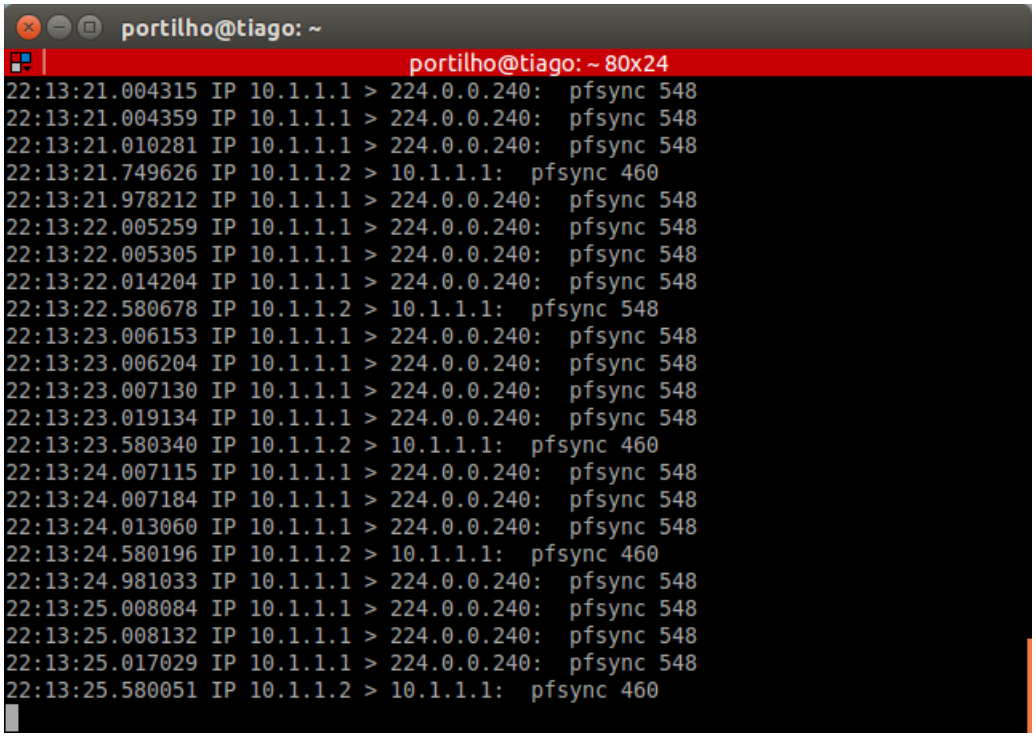


Figura 4.8 – Regras *Intranet1*.

5 CONCLUSÃO

O presente trabalho descreveu os problemas enfrentados na topologia lógica da rede de computadores do HUSM (Hospital Universitário de Santa Maria), e também uma proposta de reestruturação endereços IPv4 para a rede lógica. Tendo em vista alguns tópicos importantes como escalonamento e segurança. Em termos de escalonamento foi possível identificar que para evitar a falta de endereços IPv4 privados, é ideal criar subredes internas com prefixos pequenos o suficiente prevendo um futuro crescimento da rede. Além disso utilizar tecnologias como VLAN *(Virtual Local Area Network)*, é de extrema importância para minimizar a inundação de *broadcast* na rede.

Em termos de segurança não basta ter um *firewall* na rede, e sim uma alta disponibilidade de *firewall* bem configurado com uma política padrão adequada que seja possível interferir em todas as coneões da rede, em harmonia com o *proxy* não transparente, para ter uma opção de filtrar pacotes HTTPS interessante. O acesso das VPN restritos apenas para o destino que elas realmente precisam. Também é importante explorar alguns serviços que os *switches* disponibilizam, como *port security* e dhcp *snooping*, para evitar que usuários mal intencionados interfiram no funcionamento da rede lógica.

Para trabalhos futuros, pretende-se elaborar uma proposta de implementação de endereços IPv6*(Internet Protocol version 6)*, para a rede do hospital.

REFERÊNCIAS

CHESWICK, W. R. **Firewalls e Segurança na Internet**. 2th.ed. Porto Alegre: Bookman Companhia Editora, 2005.

CISCO. **Cisco IOS Software Configuration Guide**. Acessado em novembro/2014, http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book.pdf.

FILIPETTI, M. A. **CCNA 4.1 - Guia Completo de Estudo**. Florianópolis, Brasil: Visual Books Editora, 2008.

KUROSE, J. F.; ROSS, K. w. **Redes de computadores e a Internet**: uma abordagem top-down. 5th.ed. São Paulo: Pearson Education, Inc., 2010.

NAKAMURA, E. T.; GEUS, P. L. de. **Segurança de Redes em Ambientes Cooperativos**. São Paulo, Brasil: Novatec Editora Ltda, 2007.

OPPENHEIMER, P. **Projeto de redes top-down**. 2th.ed. Rio de Janeiro, Brasil: Editora Campus Ltda, 1999.

SOUSA, L. B. de. **Projetos e implementação de redes**: fundamentos, soluções, arquiteturas e planejamento. 3th.ed. São Paulo, Brasil: Editora Érica Ltda, 2013.

TANEBAUM, A. S.; WETHERALL, D. **Redes de computadores**. 5th.ed. São Paulo: Pearson Education, Inc., 2011.