LIGA DE ENSINO DO RIO GRANDE DO NORTE CENTRO
UNIVERSITÁRIO DO RIO GRANDE DO NORTE
ESPECIALIZAÇÃO EM REDES DE COMPUTADORES

ANDERSON BRUNO DOS SANTOS CRUZ

PROJETO DE REDE – SENAC ALECRIM

NATAL/RN
2015

ANDERSON BRUNO DOS SANTOS CRUZ

PROJETO DE REDE – SENAC ALECRIM

Monografia de conclusão de curso apresentada ao Centro Universitário do RN, como requisito final para a obtenção do título de Especialista em Redes de Computadores.

Orientador:
Profº M.Sc. Aluízio Ferreira da Rocha Neto

NATAL/RN
2015

ANDERSON BRUNO DOS SANTOS CRUZ

PROJETO DE REDE – SENAC ALECRIM

Bancada Examinadora

Aluízio Ferreira da Rocha Neto, M.Sc.
Orientador

Membro examinador

Membro examinador

NATAL/RN
2015

RESUMO

Este trabalho de conclusão de curso visa elaborar o projeto de implementação e acompanhamento de uma topologia de rede para os servidores de rede do Senac Alecrim. Com base na análise da atual situação desta rede, foi verificado a necessidade das melhorias em termos de disponibilidade, robustez e segurança, e que proporcionasse aos usuários um melhor uso da infraestrutura da unidade, bem como da conexão com a Internet. Após a implementação dos novos serviços, foi observado uma melhora significativa na qualidade do serviço prestado, como o aumento na banda para tráfegos de dados, barreiras de segurança logica e física, monitoramento inteligente da rede e também na sua disponibilidade.

Palavras chaves: Rede de Computadores, Gerenciamento de Rede.

ABSTRACT

This course conclusion work aims to develop the project implementation and monitoring of a network topology for Senac Alecrim's network servers. Based on the analysis of the current situation of this network, the need for improvements in availability has been verified, beyond robustness and security, and that would give users a better infrastructure use as well as the Internet connection. After the implementation of new services, a significant improvement was observed in the quality of service, as the increase in bandwidth for data traffic, logical security and physical barriers, intelligent network monitoring and also on their availability.

Keywords: network management; network planning, network computers, Senac Alecrim.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

O Senac Alecrim possui uma estrutura para acomodar centenas de usuários. Entre eles estão os alunos, professores e colaboradores, em diversas modalidades de cursos e de serviços. Nessa estrutura, os usuários podem acessar a Internet, alunos interagirem com os professores através de e-mails e os colaboradores acessarem suas unidades de rede e acessarem a Internet. Para garantir acesso à rede de uma forma segura e confiável, se faz necessário os requisitos técnicos mais comuns, quando se fala de redes de computadores: Disponibilidade, desempenho, segurança, gerenciabilidade, custo/benefício e adaptabilidade. Esses requisitos podem informar a qualidade da sua rede.

Para garantir os requisitos técnicos dos usuários do Senac Alecrim, foi elaborado um projeto de rede visando a melhoria na qualidade do serviço prestado, aumento da capacidade de transmissão e a segurança contra ataques externos e internos, tendo em mente as boas práticas recomendadas pela ITIL. Para identificar defeitos na rede, foi contemplado um sistema de gerenciamento de redes via SNMP. O gerenciamento de rede pode ser definido como a coordenação de recursos matérias e ou lógicos, fisicamente distribuído na rede, garantindo na medida do possível, confiabilidade, tempos da resposta aceitável e segurança da informação. Assim, o tempo para diagnóstico de falha pode ser reduzido drasticamente, evidenciando ao administrador da rede onde está ocorrendo a possível falha.

O projeto será detalhado, e a metodologia utilizada será descrita no desenvolvimento desta monografia. Este projeto é uma ferramenta operacional e gerencial, e permitirá aos administradores da rede realizar diagnósticos das falhas com alarmes, assim como análise de capacidade dos elementos por meio de gráficos de utilização. O gerente de TI receberá os relatórios gerências da disponibilidade da rede, tempo de recuperação de falhas e histórico dos alarmes.

O projeto foi elaborado visando melhorar a qualidade da rede, facilitar a monitoração utilizando plataformas de gerenciamento SNMP e proporcionando visibilidade da rede, sempre respeitando as limitações impostas, como exemplo recursos financeiros e de hardware.

1.1 OBJETIVOS

O objetivo principal desse trabalho é projetar e implantar uma nova topologia de rede no Senac Alecrim, com a finalidade de serem alcançados serviços de rede com mais disponibilidade, segurança e rapidez.

1.1.1 Objetivos Específicos

Para atingir o objetivo geral, as seguintes metas foram definidas para o projeto da nova rede:

- Aumentar a disponibilidade da rede local e acesso à Internet;
- Diminuir a vulnerabilidade da rede e servidores;
- Impedir que os dados dos usuários sejam visualizados por pessoas má intencionadas;
- Dificultar acesso não autorizado à rede ou aos servidores;
- Possibilitar a implementação de regras, serviços e políticas com os interesses da organização;
- Aumentar a satisfação dos usuários em relação aos serviços prestados e maximizar a capacidade de transmissão da rede.

1.2 ORGANIZAÇÃO DO TRABALHO

Monografia está organizada da seguinte maneira capitulo 2 mostra o referencial teórico, abordando os pontos que serão tratados nesse trabalho e a justificativa da escolha de cada um. O capitulo 3 mostra o projeto detalhado e suas especificações e a implementação da nova rede. O capítulo 4 mostra os resultados alcançados com a implantação da nova rede e o capitulo 5 conclui com as considerações finais.

2 REFERENCIAL TEÓRICO

Uma rede de computadores consiste em dois ou mais computadores e outros dispositivos interligados entre si de modo a poderem compartilhar, recursos físicos e lógicos, estes podem ser de tipo: Dados, impressora, mensagens e entre outros.

2.1 ITIL

A ITIL, *Information Technology Infrastructure Library*, ou Biblioteca de Tecnologia da informação, foi desenvolvida pela CCTA, atualmente OGC. A OGC é um órgão do governo britânico que tem como objetivo desenvolver metodologias e criar padrões dentro do departamento do governo britânico buscando otimizar e melhorar os processos internos.

A ITIL não é padrão a ser imposto, mas um conjunto de melhoras práticas que podem ser adaptadas ao setor de TI de qualquer instituição, independente de estrutura organizacional. Serve como guia para que uma instituição possa implementar as boas práticas do mercado e venha a obter melhor desempenho nas suas operações.

As atividades da ITIL são divididas em processos que cobrem as tarefas da área de TI. As boas práticas têm por objetivos servir como parâmetro para melhoria dos processos no departamento de TI.

A ITIL tem suas práticas flexíveis, aparecem com sugestões que pode sem aplicadas em diversas situações em diferentes organizações, com metodologias diferentes. O principal objetivo da aderência a ITIL é o gerenciamento de TI.

A ITIL é uma base de livros por isso o nome biblioteca. Tinha um grande conjunto de livros, cada um descrevia uma área específica de manutenção e operação de infraestrutura de TI. Sua primeira versão ITILv1 existe cerca de quarenta livros relacionados a gerenciamento da infraestrutura. A ITILv2 possui em sua biblioteca sete livros organizado é mostrada de acordo com a Figura 1.

Figura 1: Estrutura dos Livros ITIL v2

A atual versão da ITILv3 possui cinco livros. O ciclo da vida de um serviço tem como base a estratégia de serviço. A estratégia vai direcionar todas as outras partes que são desenhos de serviço, transição de serviço e operação de serviço. Envolvendo todas as partes do ciclo de vida está a melhoria do serviço continuada. Funções e processos estão distribuídos ao longo deste ciclo de vida.

- **Estratégia de Serviço**: A TI vai se interagir com o negócio, vai buscar entender as necessidades e demandas dos clientes. Encontrar pontos de risco e oportunidades, optar por terceirização de serviço ou não, pensando sempre no retorno que será gerado para o negócio.
- **Desenho do serviço:** Será projetado um novo serviço, esse serviço foi levantado na análise do passo anterior. Veremos os custos, mercado e como o serviço será utilizado. O serviço terá na estratégia o valor agregado ao cliente, pensar nos acordos de nível de serviço para performance da rede.
- **Transição do serviço:** Após o desenho, a transição criará o serviço. Nesta fase a preocupação com os detalhes para que o serviço seja colocado de forma a não impactar a organização.
- **Operações do serviço:** Manter o serviço criado na fase anterior, encontrar os processos e funções que vão conciliar com as atividades diárias.
- **Melhoria de serviço continuada:** Última parte envolve todas as outras partes citadas e possui um foco maior na qualidade, avaliando o serviço e os processos de gerenciamento dos estágios do ciclo da vida.

Se todos os estágios forem executados corretamente, ao criar ou alterar qualquer serviço teremos menos retrabalhos e teremos um controle sobre custos.

Ciclo da vida é descrito na Figura 2 e compara as versões 2 e 3 da ITIL.

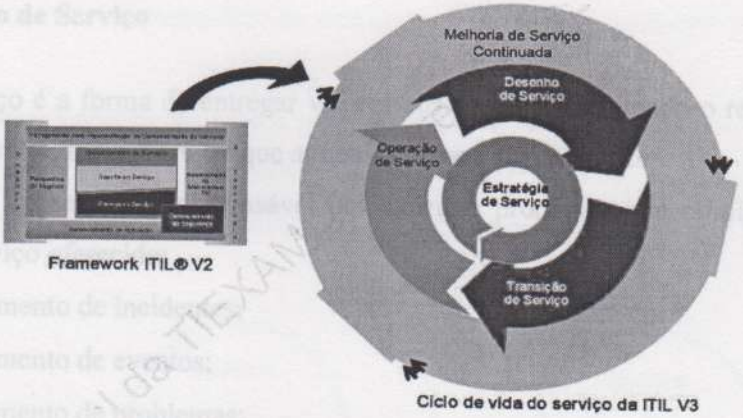


Figura 2: Ciclo de Vida ITIL v2 e ITIL v3

2.1.1 Gerenciamento de Serviços de TI

O gerenciamento de serviço na TI é conjunto de habilidades da organização em fornecer valor ao cliente, em forma de serviço. Como sugere o manual da ITIL.

Os processos da ITIL buscam a eficiência e eficácia. Duas palavras parecidas, mas com significados bem diferentes. Eficiência significa melhoria no processo, otimização e por sua vez a eficácia significa atingir os resultados esperados. Há algumas características no gerenciamento de serviço da TI que serão mostradas a seguir.

- **Gerenciamento de configuração:** Informa o gerenciamento financeiro para serviços de TI, de forma a fazer a contabilização de gastos sobre os ativos de TI. Ativo pode possuir valor e depreciação.
- **Gerenciamento de Mudança:** Levanta os aspectos referentes as mudanças.
- **Gerenciamento de Liberação:** Com as informações levantadas no gerenciamento de configuração e no gerenciamento de mudança, registra as liberações instaladas no ambiente de produção.
- **Gerenciamento de Incidente:** Funciona em conjunto com os processos de gerenciamento de problema e gerenciamento de mudança.
- **Gerenciamento de Problemas:** É implementado após o processo de gerenciamento de incidente.
- **Gerenciamento de Nível de Serviço:** Importante ter implementado o serviço de suporte para dar suporte aos acordos nos níveis de serviços.
- **Gerenciamento de Capacidade:** Assegura a capacidade da infraestrutura de TI esteja de acordo com as necessidades do negócio.

2.1.2 Operação de Serviço

Um serviço é a forma de entregar valores aos clientes, facilitando o resultado que os clientes pretendem alcançar. Sem ter que assumir custos e riscos. ITILv3.

Operação de serviço é responsável por executar processos que otimizam o custo e qualidade do serviço oferecido:

- Gerenciamento de incidentes;
- Gerenciamento de eventos;
- Gerenciamento de problemas;
- Cumprimento de requisitos;
- Gerenciamento de acessos;

2.2 REDES VIRTUAIS

O conceito de VLAN é uma facilidade de operação em uma rede comutada. Esta facilidade permite que o administrador configure a mesma como sendo uma única entidade interligada, enquanto são assegurados aos usuários a conectividade e a privacidade como se estivessem em multiplicas redes separas.

É possível criar redes totalmente separas para os setores acadêmicos e administrativos dentro do mesmo ambiente físico, aplicando políticas de segurança para os grupos, utilizando as VLANs. A principal característica para uso de VLANs é a possibilidades de agrupar estações pertencentes a uma ou mais LANs físicas, de forma a criar um único domínio de broadcast, garantindo a comunicação entre as LANs, mesmo que façam parte de segmentos físicos diferentes.

Uma rede não segmentada, computadores, impressoras e outros dispositivos conectados disseminam uma grande quantidade de pacotes broadcast por diversos motivos, falhas nas conexões dos cabos, mau funcionamento da interface de rede ou até mesmo por protocolos e aplicações que geram esse tipo de trafego, causando atraso no tempo de resposta e lentidão na rede local.

A implementação de VLANs para segmentar a rede melhora a performance e diminui o número de estações que compartilham o mesmo canal logico, reduzindo assim o tempo de acesso.

A segurança é uma das características mais importante quando segmentamos a rede em VLANs, já que ela permite que dispositivos localizados em diferentes segmentos físicos,

mas em uma mesma VLAN comunique-se sem que o dispositivo fisicamente próximo tenham acesso.

O roteamento entre as VLANs é necessário para que um dispositivo de uma VLAN precise se comunicar com outro dispositivo de outra VLAN. Esse roteamento pode ser feito por meio de switch de camada 3 ou utilizando um roteador, como mostrado na Figura 3.

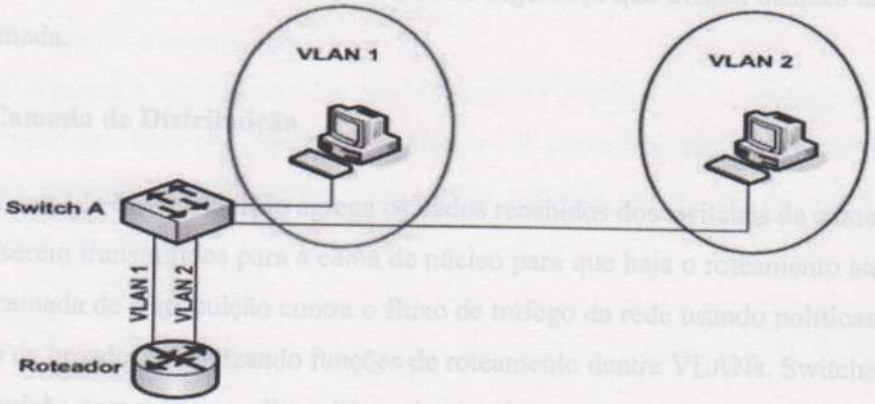


Figura 3: Roteamento entre VLANS

2.3 MODELO DE REDE HIERÁRQUICA

Uma rede hierárquica é uma divisão da rede em camadas discretas. Cada camada fornece funções especificas que definem sua função dentro da rede geral.

O modelo de uma rede hierárquica típico é divido em três camadas: acesso, distribuição e núcleo, conforme é mostrado na Figura 4.

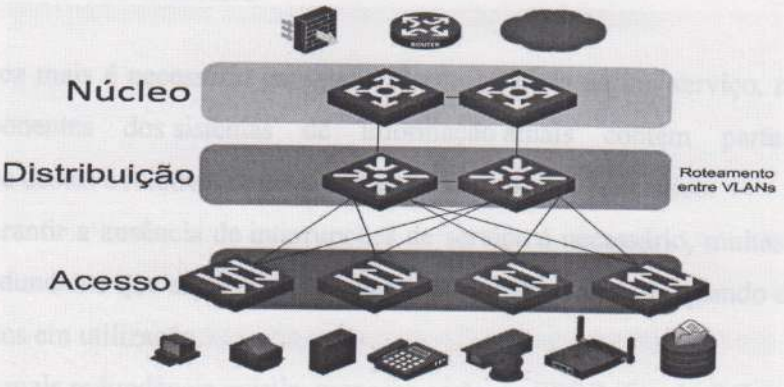


Figura 4: Diagrama de uma rede hierárquica

2.3.1 Camada de Acesso

A Camada de Acesso faz a interface com dispositivos finais, como computadores, impressoras, telefones IP, para fornecer acesso ao restante da rede.

Na camada de acesso também podemos encontrar, switches, hubs, roteadores e AP. O objetivo principal da camada de acesso é conectar dispositivos a rede e controlar quem vai ter permissão de comunicação na rede. Políticas de segurança que evitam ataques também ficam nessa camada.

2.3.2 Camada de Distribuição

A camada de distribuição agrega os dados recebidos dos switches da camada de acesso antes de serem transmitidos para a cama de núcleo para que haja o roteamento até seu destino final. A camada de distribuição contra o fluxo de tráfego da rede usando políticas e determina domínios de broadcast, realizando funções de roteamento dentre VLANs. Switches da camada de distribuição costumam ser dispositivos de alto desempenho que tem alta disponibilidade e redundância para assegurar a confiabilidade.

2.3.3 Camada de Núcleo

A camada de núcleo na rede hierárquica é o backbone de alta velocidade das redes interconectadas, como a camada de núcleo é essencial a interconectividade entre os dispositivos da camada de distribuição, é importante que o núcleo seja altamente disponível e redundante. A área de núcleo também pode se conectar a recursos de internet e deve ser capaz de encaminhar grandes quantidades de dados rapidamente.

2.4 ALTA DISPONIBILIDADE

Cada vez mais é necessário garantir a disponibilidade de um serviço, mas sendo que muitos componentes dos sistemas de informação atuais contêm partes mecânicas, a confiabilidade destes é relativamente insuficiente se o serviço for crítico.

Para garantir a ausência de interrupções de serviço é necessário, muitas vezes, dispor de hardware redundante que entre em funcionamento automaticamente quando da falha de um dos componentes em utilização.

Quanto mais redundância existir, menores serão os SPOF (Single Point Of Failure), e menor será a probabilidade de interrupções no serviço.

2.5 AUTENTICAÇÃO

Autenticação é o processo pelo qual em uma comunicação cada parte verifica seu parceiro é quem deveria ser e não imposto. Por meio da autenticação será possível identificar usuários que acessam ou tenta acessar serviços não autorizados pelas políticas de segurança.

É de grande relevância no processo de gestão da informação a proteção dos dados e dos recursos envolvidos nele, de modo a garantir a acesso, alteração e liberação apenas por pessoas devidamente autorizadas.

A segurança da informação está fortemente relacionada a administração moderna representando um bem que por sua vez precisa ser protegido, visando minimizar riscos no tocante ao extravio de informação, apoiando os retornos envolvidos de modo a garantir a continuidade dos negócios.

2.5.1 Proxy

Procurador, como o próprio nome já diz na sua tradução, o proxy é quem faz as requisições em nome do usuário para algum site da WEB. Tem duas funções principais: alterar as requisições ou respostas dos servidores e armazenamento temporário de dados.

Quando o proxy faz as alterações de requisições ele está agindo baseado na configuração de acesso, caso o usuário esteja autenticado e autorizado a visualização de um pagina será mostrado normalmente, caso não esteja autorizado o proxy direciona para outra página ou mostra a página de bloqueio.

O armazenamento temporário de dados é conhecido com cache, quando um usuário faz uma requisição o proxy armazena essa informação localmente, como isso pode ser recuperada rapidamente ao invés de ir buscar novamente a mesma requisição, além de deixar a banda disponível para atender outras requisições mais rapidamente.

2.6 FIREWALL

Firewall é uma solução de segurança baseada em hardware ou software que, a partir de um conjunto de regras ou instruções, analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas. "Parede de fogo", a tradução literal do nome, já deixa claro que o firewall se enquadra em uma espécie de barreira de defesa. A sua missão, por assim dizer, consiste basicamente em bloquear tráfego de dados indesejado e liberar acessos bem-vindos.

Firewall atua como uma espécie de barreira que verifica quais dados podem passar ou não. Esta tarefa só pode ser feita mediante o estabelecimento de políticas, isto é, de regras.

2.7 GERÊNCIA

É necessário gerenciar os recursos e serviços relacionados ao desempenho e disponibilidade da rede.

Implementação de um servidor de monitoramento para o controle sobre os elementos da rede, sendo eles físicos e lógicos, assim garantindo a continuidade e qualidade dos serviços oferecidos.

2.7.1 Monitoramento

Monitorar é observar, analisar e ficar atento aos possíveis sinais de que algo não está normal. Em tecnologia da informação, "não está normal" pode indicar indisponibilidade de um ou mais partes de um sistema ou mesmo uma lentidão ou diminuição na qualidade de serviços percebida pelo cliente. Estar pronto para ação, ou mesmo agir antes de algo acontecer, são resultados de um bom ambiente de monitoramento de redes, servidores e serviços. Além disso, os dados históricos coletados por um bom sistema de monitoramento fornecem informações para que compras e upgrades sejam feitos de forma racional (Capacity Planning).

As ferramentas de monitoramento permitem que métricas sejam apresentadas de forma visual com gráficos e mapas. Informações como consumo de banda, CPU, memória, ou tempo de consultas do banco de dados, podem ser rapidamente visualizadas, tanto com dados instantâneos como para dados históricos. Um bom sistema de monitoramento de redes permite a criação de alertas para eventos de anormalidade e também permitem correlacionar sintomas com itens de infraestrutura.

Outra característica de um bom sistema de monitoramento é que ele deve ser suficiente para atender as mais diversas equipes, ambientes e necessidades, de modo a evitar que múltiplas ferramentas sejam usadas, dificultando correlações e tornando o ambiente ainda mais complexo.

3 PROJETO DA NOVA REDE

Será mostrado a seguir os requisitos estabelecidos pelos responsáveis pela rede do Senac Alecrim e as definições para a criação de uma nova rede.

3.1 TOPOLOGIA GERAL DA REDE

A topologia geral proposta para a nova rede é a apresentada na Figura 5. Essa nova topologia foi criada de acordo com a necessidade da rede e dos equipamentos que existiam. Essa topologia apresenta redundância, entre os switches de acesso e o de distribuição, além de dois firewalls, evitando assim um único ponto de falha. A utilização do protocolo RSTP previne a criação de *loops* na rede e sua reconfiguração é rápida em caso perda de um dos links.

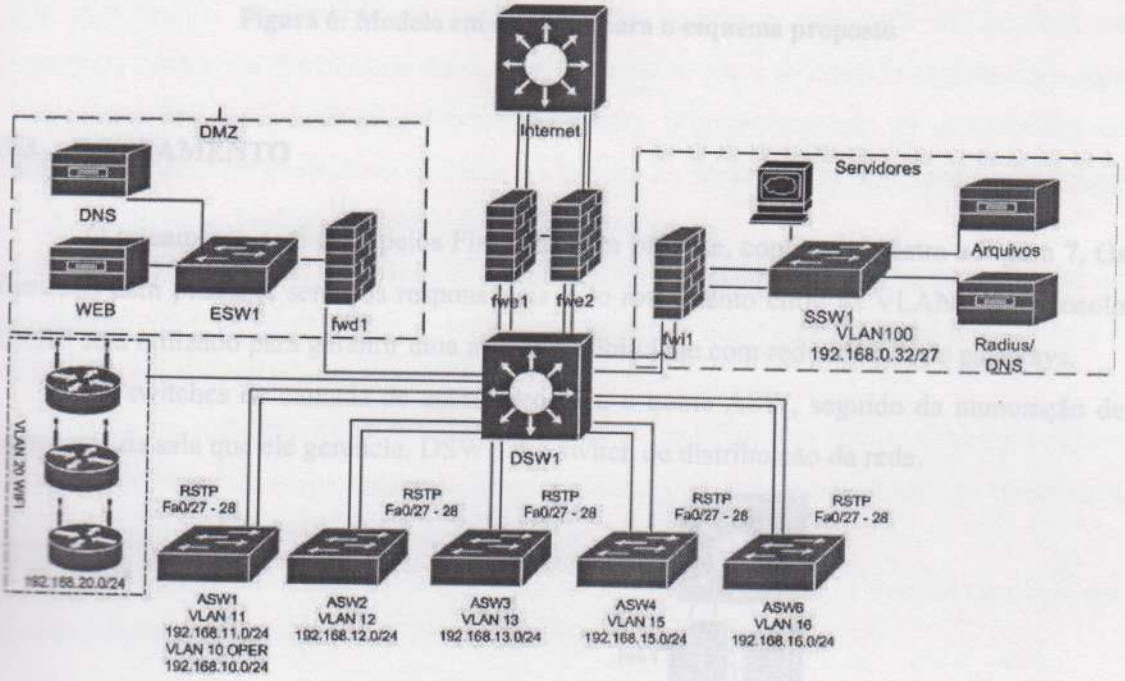


Figura 5: Topologia geral da nova rede

A rede foi segmentada em VLANs, para diminuir o trafego de broadcast. Após a segmentação da rede os servidores ficaram isolados do restante da rede, isso para impedir acessos indevidos, com isso todas as conexões passaram pelo firewall.

3.2 ESTRUTURA DE REDE LOCAL

A estrutura proposta para a nova rede LAN está representada na Figura 6. Na camada de acesso estarão instalados os switches utilizados pelos usuários, e o switch de distribuição, com maior capacidade de transmissão, fará a interconexão das redes de acesso.

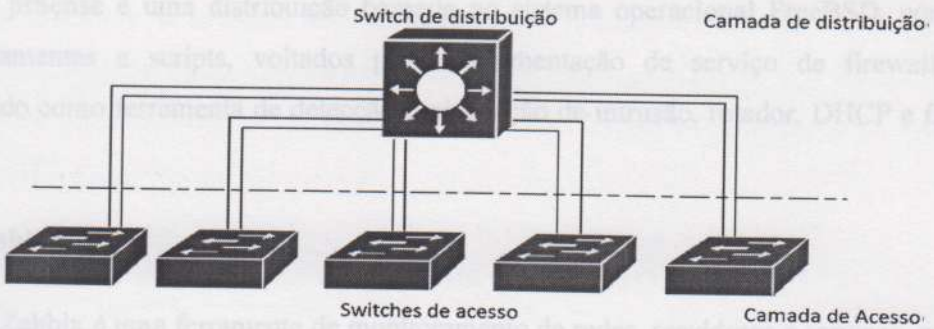


Figura 6: Modelo em camadas para o esquema proposto

3.3 ROTEAMENTO

O roteamento será feito pelos Firewalls com pfSense, conforme mostra a Figura 7. Os firewalls com pfSense, serão os responsáveis pelo roteamento entre as VLANs, o protocolo CARP será utilizado para garantir uma alta disponibilidade com redundância de gateways.

Os switches de camada de acesso recebem o nome ASW, seguido da numeração de referência da sala que ele gerencia. DSW 1 é o switch de distribuição da rede.

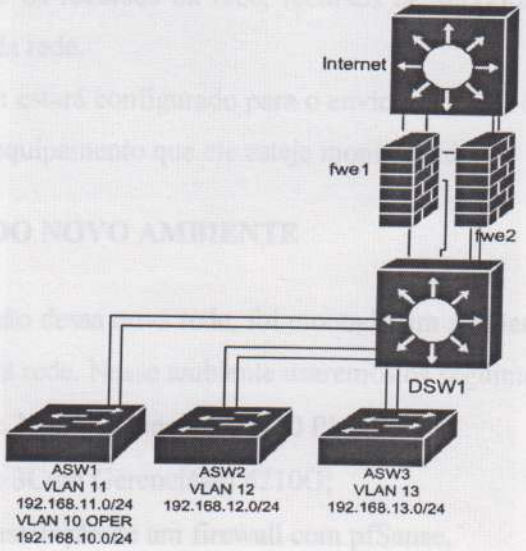


Figura 7: Esquema de roteamento e divisão das VLANS

3.4 SISTEMAS

Nesta seção serão apresentados os sistemas propostos para os servidores de rede.

3.4.1 pfSense

O pfSense é uma distribuição baseada no sistema operacional FreeBSD, composto com ferramentas e scripts, voltados para implementação de serviço de firewall. Será configurado como ferramenta de detecção e prevenção de intrusão, rotador, DHCP e firewall DNS.

3.4.2 Zabbix

O Zabbix é uma ferramenta de monitoramento de redes, servidores e serviços, pensada para monitorar a disponibilidade, experiência de usuário e qualidade de serviços. A arquitetura Zabbix e a flexbilidade dos módulos permitem que a ferramenta seja utilizada para o monitoramento convencional (vivo/morto on/off), acompanhamento de desempenho de aplicações, análise de experiência de usuário e análise de causa raiz em ambientes complexos, através do servidor Zabbix e as regras de correlacionamento.

Através do uso do protocolo de monitoramento e gerenciamento de rede SNMP, os switches de distribuição e de firewall serão monitorados, e o uso do ICMP será para conferir o estado dos switches de acesso.

Com as informações coletadas serão criados gráficos em tempo real para serem monitorados visualmente os recursos da rede, recursos de servidores, o tráfego referente a cada sala e mapa visual da rede.

O Zabbix também estará configurado para o envio automático de e-mails alertando em caso de falha em algum equipamento que ele esteja monitorando.

3.5 PREPARAÇÃO DO NOVO AMBIENTE

Para implementação dessa nova rede, foi montado um ambiente para elaboramos teste de funcionamento da nova rede. Nesse ambiente usaremos os seguintes equipamentos:

- Switch Camada 2: 3Com Gerenciável 2250 Plus;
- Switch Camada 3: 3Com Gerenciável 4210G;
- Computador I3: Instalação de um firewall com pfSanse.

3.6 IMPLEMENTAÇÃO DA NOVA REDE

As configurações que serão realizadas nesses equipamentos serão mostradas a seguir.

3.6.1 Configuração dos Switches Para Suporte a VLANs

Na nova rede os firewalls externos irão fazer o roteamento entre as VLANs e a rede externa e roteamento local. O Gateway Default de todas as VLANs é o FWE1(firewall externo 1) ou (firewall externo 2), caso o primeiro falhe. Segue a configuração do Switch de Acesso ASW1.

```
System/Fabric Name: ASW1
System Location: Switch para atender LAB 104 e administração
IP Address Assigment - Manual
IP Address - 192.168.0.1
Subnet Mask - 255.255.255.254
Default Gateway - 192.168.0.10
VLAN11 - Portas Fast 0/1 a 35 - LAB 104
VLAN10 - Portas Fast0/35 a 48 - Administração
```

3.6.2 Configuração do DSW1 na Porta do Firewall

No switch de distribuição as portas em que o firewall fica conectado ficam configuradas como *tagged* para todas as VLANs, menos para a VLAN que a porta do firewall faça parte. A Figura 8 mostra a tela de configuração do switch de distribuição.

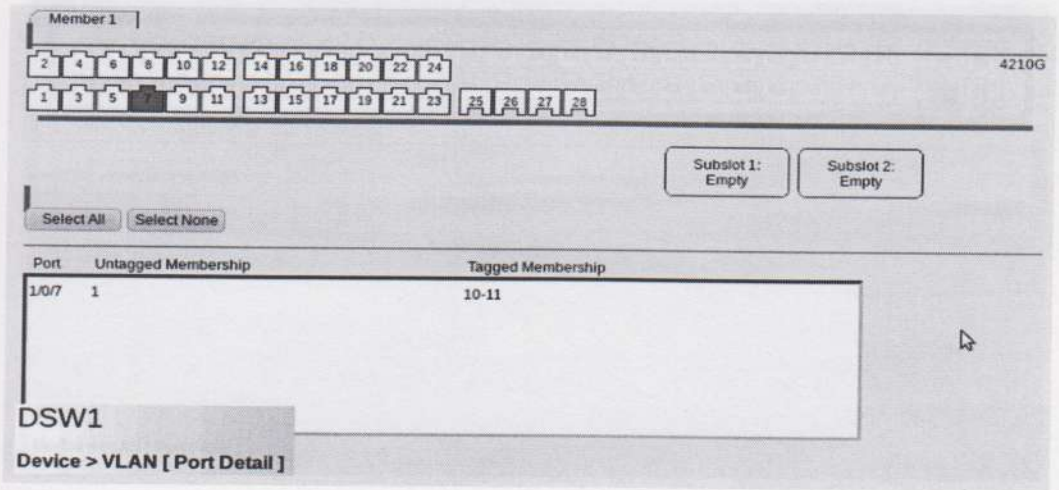


Figura 8: Configuração do Switch de Distribuição

3.6.3 Conexão entre DSW1 e os demais switches de acesso

As portas de conexões do DSW1 com os demais switches devem se comunicar entre as VLANs configuradas nos equipamentos de acesso e com o restante da rede. Para isso acontecer a portas do DSW1 e ASWX devem estar configuradas com tagged para todas as VLANs do switch de acesso. A Figura 9 mostra a configuração do switch de distribuição.

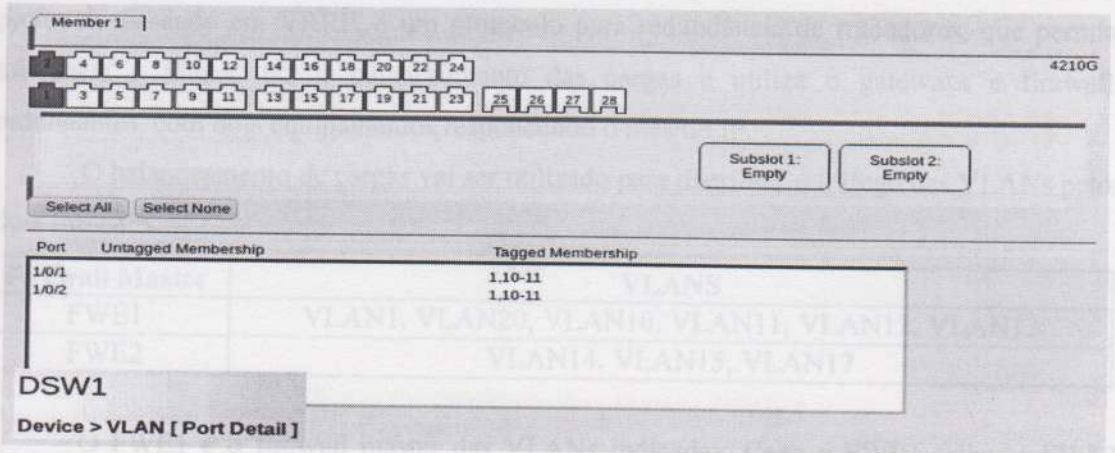


Figura 9: Configuração do switch de distribuição com partas tagged.

Na Figura 9, é mostrada a configuração do switch de distribuição, procedimento deve ser o mesmo no comutador da rede de acesso, como mostrado na Figura 10.

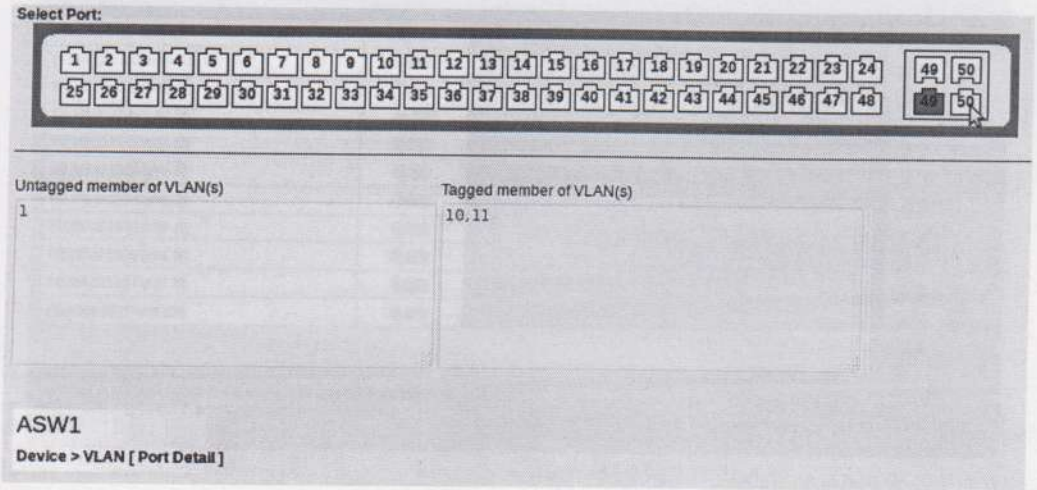


Figura 10: Configuração do switch de acesso

Como sugere a ITIL é importante reduzir os riscos que possam afetar o bom funcionamento do negócio, por isso foi incluído redundância nos pontos críticos da rede, a redundância é garantida pelo protocolo RSTP.

3.6.4 Implementação de Cluster de Firewall com CARP

A implementação de dois firewalls externos com redundância com CARP. CARP protocolo baseado em VRRP, é um protocolo para redundância de roteadores, que permite tolerância a falhas, faz o balanceamento das cargas e utiliza o gateways e firewalls redundantes, com dois equipamentos respondendo o mesmo IP.

O balanceamento de cargas vai ser utilizado para distribuir o tráfego das VLANs pelos dois firewalls.

Firewall Master	VLANS
FWE1	VLAN1, VLAN20, VLAN10, VLAN11, VLAN12, VLAN13
FWE2	VLAN14, VLAN15, VLAN17

O FWE1 é o firewall master das VLANs indicadas. Caso o FWE1 falhe, o FWE2 assume automaticamente o trafego de todas as redes e vice-versa. Na Figura 11 mostra a tela de configuração do firewall com o CARP.

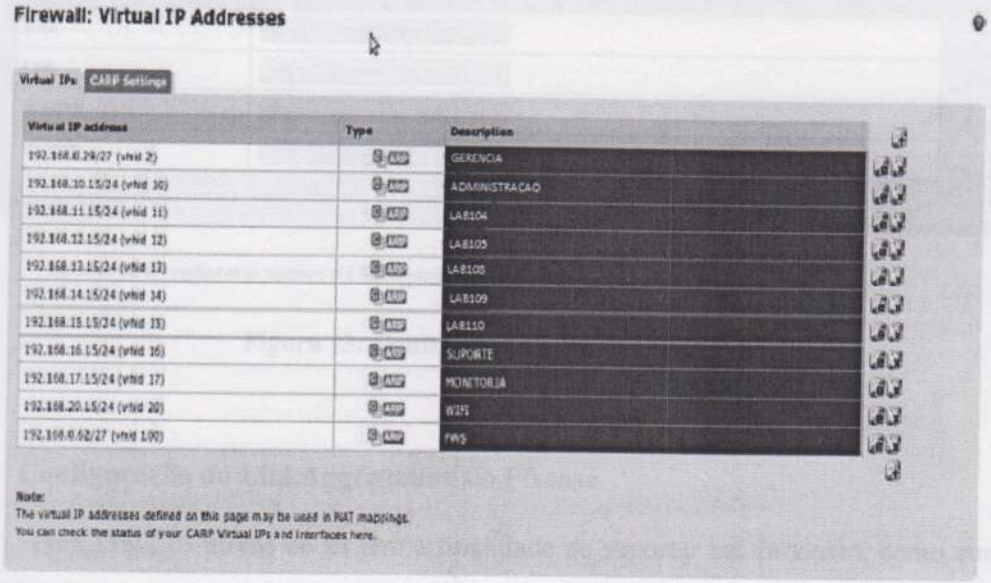


Figura 11: Configuração do pfSense - CARP

3.6.5 Servidor DHCP no pfSense

O pfSense tem uma característica funciona como servidor DHCP, apenas para interfaces que estejam configuradas no mesmo. É necessário criar uma VLAN e associar ao link LAN para cada subrede. Conforme exemplo das Figuras 12 e 13.

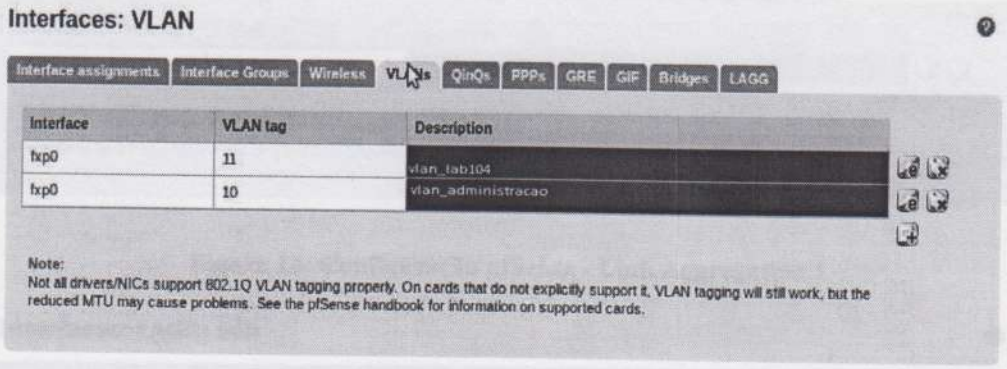


Figura 12: Configuração pfSense - DHCP 1

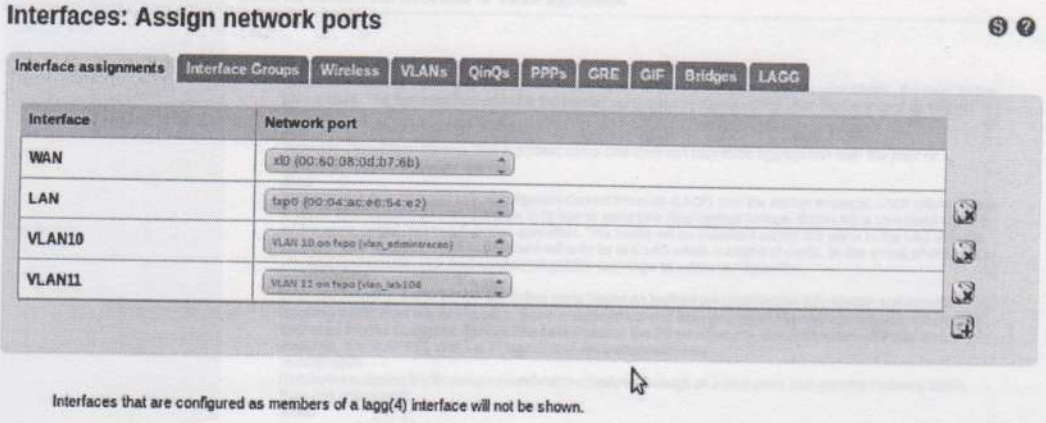


Figura 13: Configuração pfSense - DHCP 2

3.6.6 Configuração do LinkAggregation no Pfsense

Para ITIL, os ativos de TI têm a finalidade de suportar um processo, como aumento da banda. Com o aumento da banda haverá maior disponibilidade, qualidade e capacidade para os usuários e neste caso diminui a indisponibilidade de banda.

O linkAggregation permite a utilização de várias portas ethernet agrupadas, com isso forma um único link, proporcionando o aumento da banda e redundância em casa de falha. As Figuras 14 e 15 mostram a configuração do LinkAggegation no pfSense.

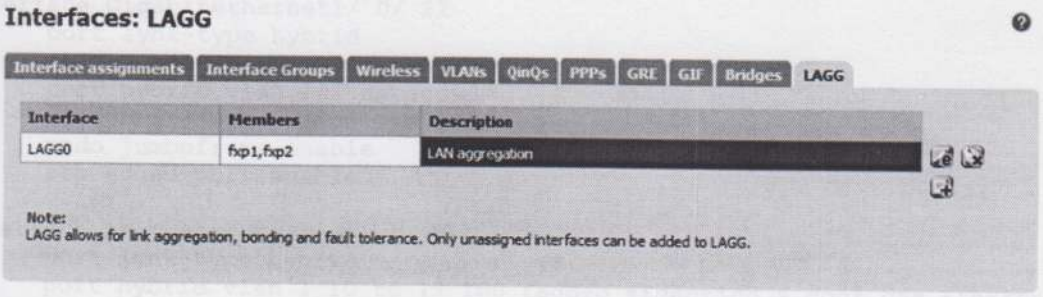


Figura 14: Configuração pfSense - Link Aggregation 1

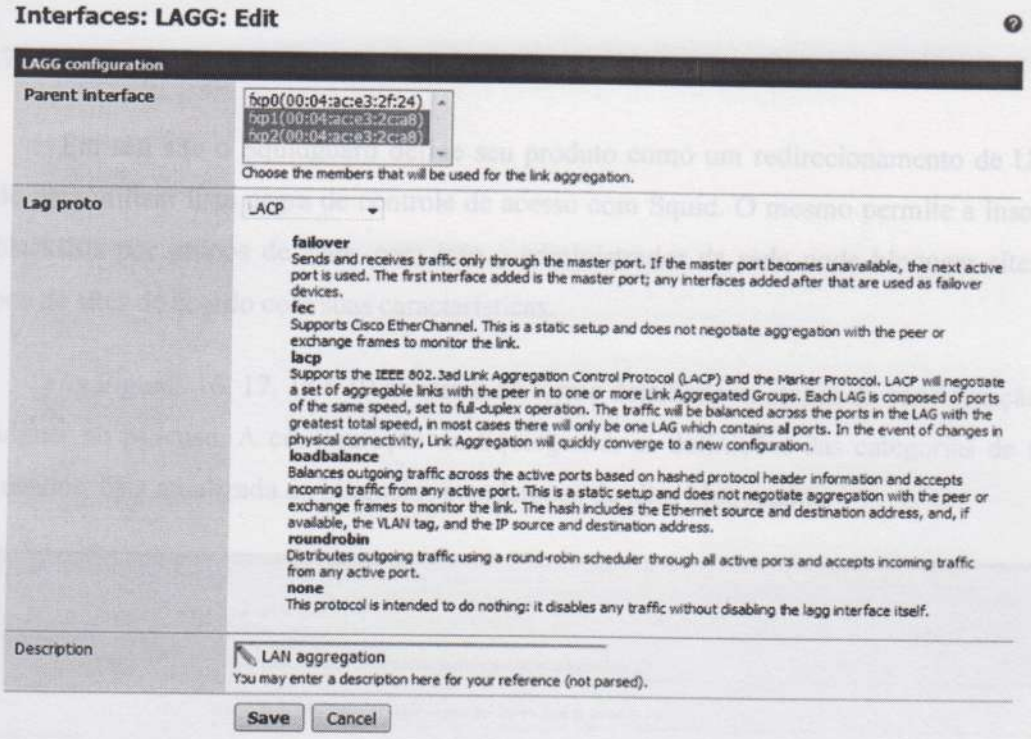


Figura 15: Configuração pfSense - Link Aggregation 2

As interfaces que forem escolhidas necessariamente devem estar sem IP configurado. O LACP será o protocolo utilizado. No switch, o protocolo precisa ser o mesmo e a interface BridgeAggregation precisa estar configura com o mesmo tipo de porta e VLANs liberadas nos seus links Gigabitethernet, segue a configuração:

```
Interface Gigabitethernet1/ 0/ 21
     port lynk-type hybrid
```

```
      port hybrid vlan 1 10 to 17 100 tagged
      port hybrid vlan 101 untagged
      broadcast-suppression pps 3000
            undo jumboframe enable
      stp edged-port enable

Interface Gigabitethernet1/ 0/ 22
      port lynk-type hybrid
      port hybrid vlan 1 10 to 17 100 tagged
      port hybrid vlan 101 untagged
      broadcast-suppression pps 3000
      undo jumboframe enable
      stp edged-port enable

Interface BridgeAggregation1
      port lynk-type hybrid
      port hybrid vlan 1 10 to 17 100 tagged #idêntico a conf das Ethernets
      port hybrid vlan 101 untagged          #idêntico a conf das Ethernets
      link-aggregation mode dynamic          #negocia automaticamente com FEW
```

3.6.7 Implementação do Squidguard

Em seu site o Squidguard define seu produto como um redirecionamento de URLs usado para utilizar lista negra de controle de acesso com Squid. O mesmo permite a inserção de blacklists por grupos de sites, com isso o administrador da rede pode bloquear sites ou grupos de sites de acordo com suas características.

As Figuras 16, 17, 18 e 19 mostram de forma detalhada as etapas da configuração do Squidguar no pfSense. A configuração do Squidguard, as definições das categorias de sites bloqueados, lista atualizada de bloqueios e endereços de sites bloqueados.

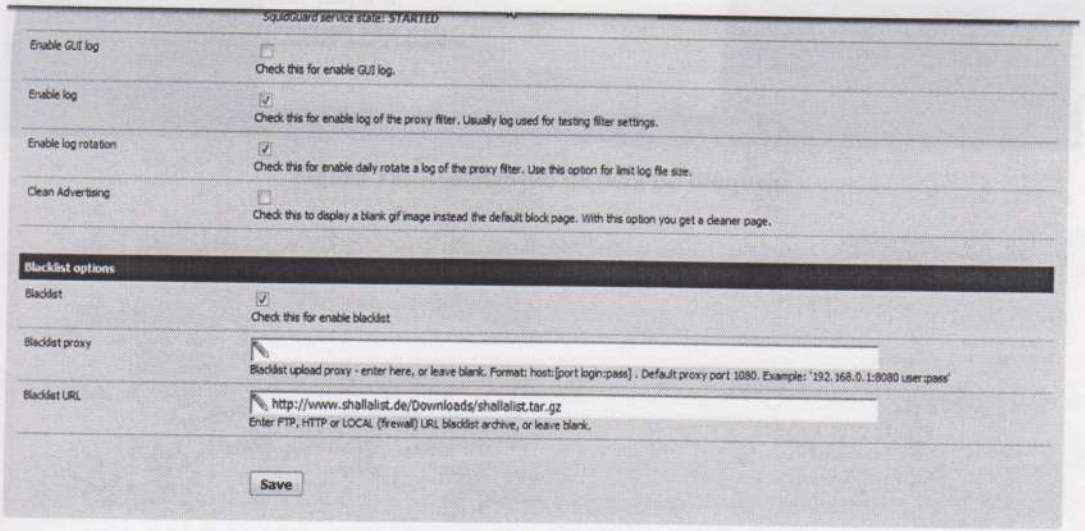


Figura 16: Configuração do pfSense - Squidguard

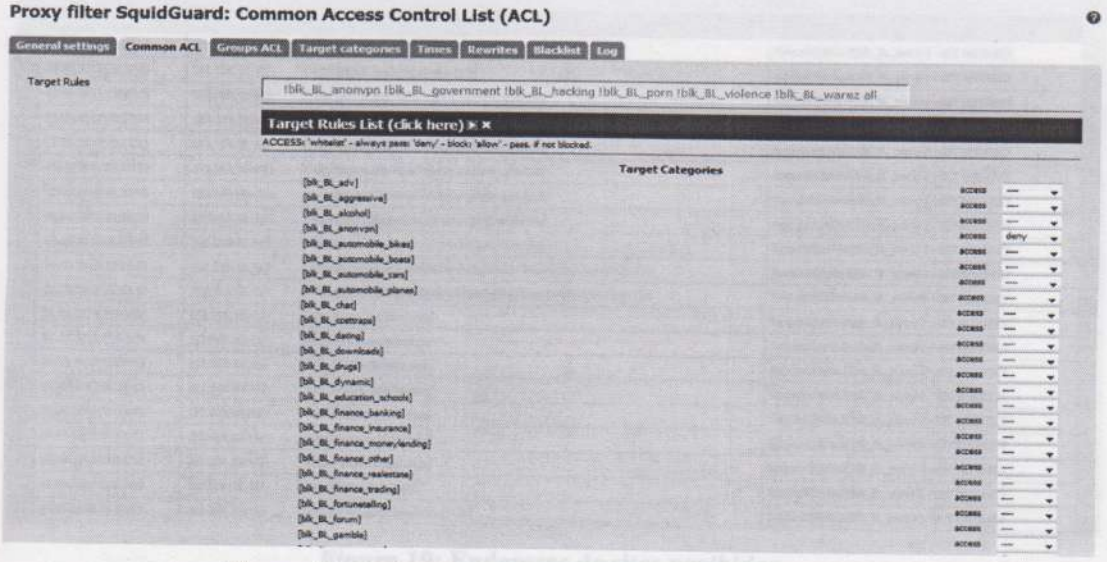


Figura 17: Definições das categorias de sites bloqueados

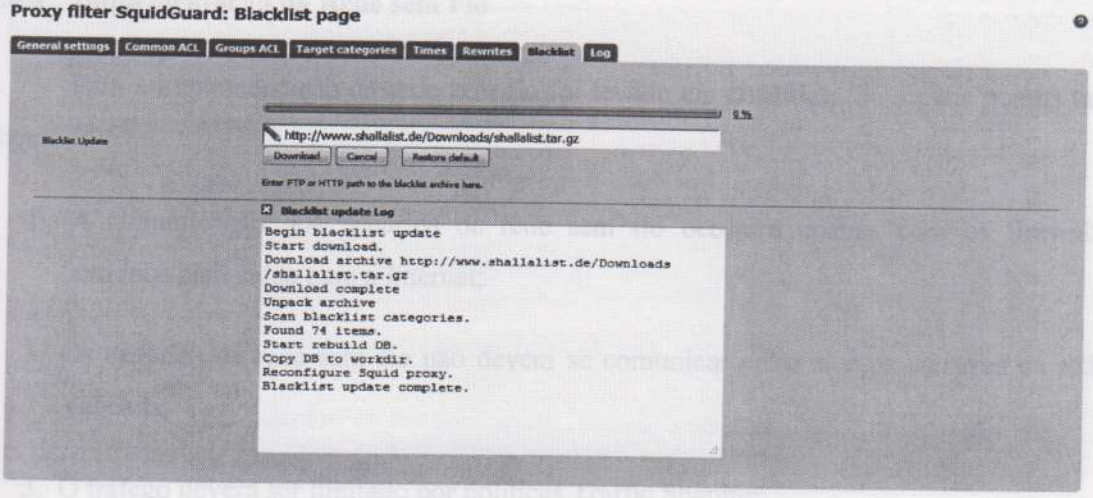


Figura 18: Atualização de lista de bloqueio

Proxy filter SquidGuard: Log page

General settings | Common ACL | Groups ACL | Target categories | Times | Rewrites | Blacklist | Log

| Blocked | Filter GUI log | Filter log | Proxy config | Filter config |

Show top 50 entries. List from the line: << 0 >>

29.08.2012 22:24:00	192.168.10.41/-	http://www.xvideos.com/tags/putaria	Request(default/blk_BL_porn/-) - GET REDIRECT
29.08.2012 22:23:43	192.168.10.41/-	http://www.putariabrasileira.com/	Request(default/blk_BL_porn/-) - GET REDIRECT
29.08.2012 22:23:33	192.168.10.41/-	http://www.kporno.com/www.redtube.com.html	Request(default/blk_BL_porn/-) - GET REDIRECT
29.08.2012 22:23:23	192.168.10.41/-	http://www.filmesporno.com/	Request(default/blk_BL_porn/-) - GET REDIRECT
29.08.2012 22:21:11	192.168.10.41/-	http://www.kporno.com/www.redtube.com.html	Request(default/blk_BL_porn/-) - GET REDIRECT
29.08.2012 22:19:53	192.168.10.41/-	http://www.kporno.com/www.redtube.com.html	Request(default/blk_BL_porn/-) - GET REDIRECT
29.08.2012 22:18:40	192.168.10.41/-	http://www.kporno.com/www.redtube.com.html	Request(default/blk_BL_porn/-) - GET REDIRECT
29.08.2012 22:18:14	192.168.10.41/-	http://www.kporno.com/www.redtube.com.html	Request(default/blk_BL_porn/-) - GET REDIRECT
29.08.2012 22:14:47	192.168.10.41/-	http://www.kporno.com/www.redtube.com.html	Request(default/blk_BL_porn/-) - GET REDIRECT
29.08.2012 22:14:37	192.168.10.41/-	http://videoporno.com/www-redtube-com-free-young-teen-fuck-.htm	Request(default/blk_BL_porn/-) - GET REDIRECT
29.08.2012 22:13:10	192.168.10.41/-	http://videoporno.com/www-redtube-com-free-young-teen-fuck-.htm	Request(default/blk_BL_porn/-) - GET REDIRECT
29.08.2012 22:12:55	192.168.10.41/-	http://www.redtube.com/	Request(default/blk_BL_porn/-) - GET REDIRECT
29.08.2012 22:07:04	192.168.10.41/-	http://www.redtube.com/	Request(default/blk_BL_porn/-) - GET REDIRECT
29.08.2012 22:07:01	192.168.10.41/-	http://www.redtube.com/	Request(default/blk_BL_porn/-) - GET REDIRECT
29.08.2012 21:56:39	192.168.10.41/-	http://www.redtube.com/	Request(default/blk_BL_porn/-) - GET REDIRECT
29.08.2012 21:54:16	192.168.10.41/-	http://www.redtube.com/	Request(default/blk_BL_porn/-) - GET REDIRECT
29.08.2012 21:54:11	192.168.10.41/-	http://www.redtube.com/	Request(default/blk_BL_porn/-) - GET REDIRECT
29.08.2012 21:53:53	192.168.10.41/-	http://www.redtube.com/	Request(default/blk_BL_porn/-) - GET REDIRECT
29.08.2012 21:53:05	192.168.10.41/-	http://www.porn.com/	Request(default/blk_BL_porn/-) - GET REDIRECT
29.08.2012 21:53:01	192.168.10.41/-	http://www.porn.com/favicon.ico	Request(default/blk_BL_porn/-) - GET REDIRECT

Figura 19: Endereços de sites proibidos

3.6.8 Implementação da Rede sem Fio

Para a implementação da rede sem fio foi levado em consideração alguns pontos tais como:

1. A comunicação dos usuários de rede sem fio ocorrera apenas com os firewalls externos para saída para a internet;
2. Os usuários da rede sem fio não devem se comunicar entre si e os usuários da rede cabeada;
3. O trafego deverá ser limitado por politicas Traffic Shaping;
4. A rede sem fio não terá acesso aos servidores da rede 100 e elementos da rede cabeada.

Na rede sem fio serão utilizados Wirelles AP, onde o servidor DHCP é centralizado.

Será usado em cada Wireless AP, o sistema operacional DD-WRT e os procedimentos usados para configuração foram retirados do site http://www.dd-wrt.com/wiki/index.php/Wireless_access_point. Segue o texto retirado do site mencionado. A Figura 20 mostra o os passos para a configuração do AP.

```
Here's how to create a Wireless Access Point using dd-wrt v24. Please pay special
attention to the Review section of this article, especially if you are using an
older version.
    1. Hard reset or 30/30/30 the router to dd-wrt default settings
    2. Connect to the router @ http://192.168.1.1
        *Note: If this router is wired to another router, there may be conflicts
 (both routers could have the same IP address).

For the time being, disconnect this router from the main one.
    3. Open the Setup -> Basic Setup tab
        WAN Connection Type: Disabled
        Local IP Address: 192.168.1.2 (i.e. different from primary router and out
 of DHCP
pool)
        Subnet Mask: 255.255.255.0 (i.e. same as primary router)
        DHCP Server: Disable (also uncheck DNSmasq options)
        (Recommended) Gateway/Local DNS: IP address of primary router (many things
 will fail without this)
        (Optional) Assign WAN Port to Switch (visible only with WAN Connection Type
set to disabled): Enable this if you want to
use WAN port as a switch port
        (Optional) NTP Client: Enable/Disable (if Enabled, specify Gateway/Local
DNS above)
        Save
    4. Open the Setup -> Advanced Routing tab
        (Optional) Change operating mode to: Router
        Save
    5. Open the Wireless -> Basic Settings tab
        Wireless Network Name (SSID): YourNetworkNameHere
        (Optional) Sensitivity Range: The max distance (in meters) to clients x2
        Save
    6. Open the Wireless -> Wireless Security tab
        Note: Security is optional, but recommended! Clients must support whatever
mode you select here.
        (Recommended) Security Mode: WPA2
        (Recommended) WPA Algorithm: AES
        (Recommended) WPA Shared Key: >8 characters
        Save
    7. Open the Services -> Services tab
        (Optional) DNSMasq: Disable (enable if you use additional DNSMasq settings)
        (Optional) ttraff Daemon: Disable
        Save
    8. Open the Security -> Firewall tab
        Uncheck all boxes except Filter Multicast
        Save
        Disable SPI firewall
        Save
    9. Open the Administration -> Management tab
        (Recommended) Info Site Password Protection: Enable
        (Recommended) Routing: Disabled (enable if you need to route between
interfaces)
        Apply Settings and connect Ethernet cable to main router via LAN-to-LAN
uplink*
    Notes:
        1. To connect the WAP to the main router, you can probably use either
a patch cable, straight-thru, or a crossover cable. Most DD-WRT capable devices
can do auto-sensing so the cable type doesn't usually matter.
        2. You can connect the WAP to the main router via LAN-to-WAN so long
as you have assigned the WAN port to switch (see step 3).
```

Figura 20: Configuração AP dd-wrt

3.6.9 Zabbix

O Zabbix será utilizado com ferramenta de monitoramento de redes, servidores e serviços, pensada para monitorar a disponibilidade, experiência de usuário e qualidade de serviços.

3.6.9.1 Criação de Hosts

Para a criação de um novo hots para ser monitorado no Zabbix, deve-se clicar em *configuration => host => Create Host*, como mostra a Figura 21.

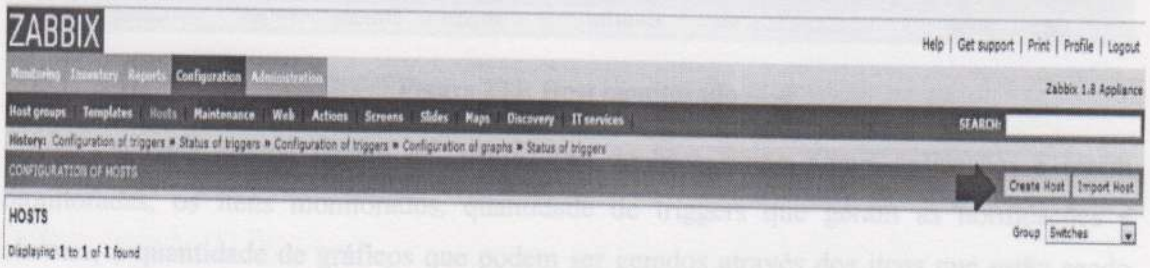


Figura 21: Criação de um novo Host

A informação do host é preenchida, com a seguintes informações: Nome, Grupo, IP e *Template*. De acordo a Figura 22.

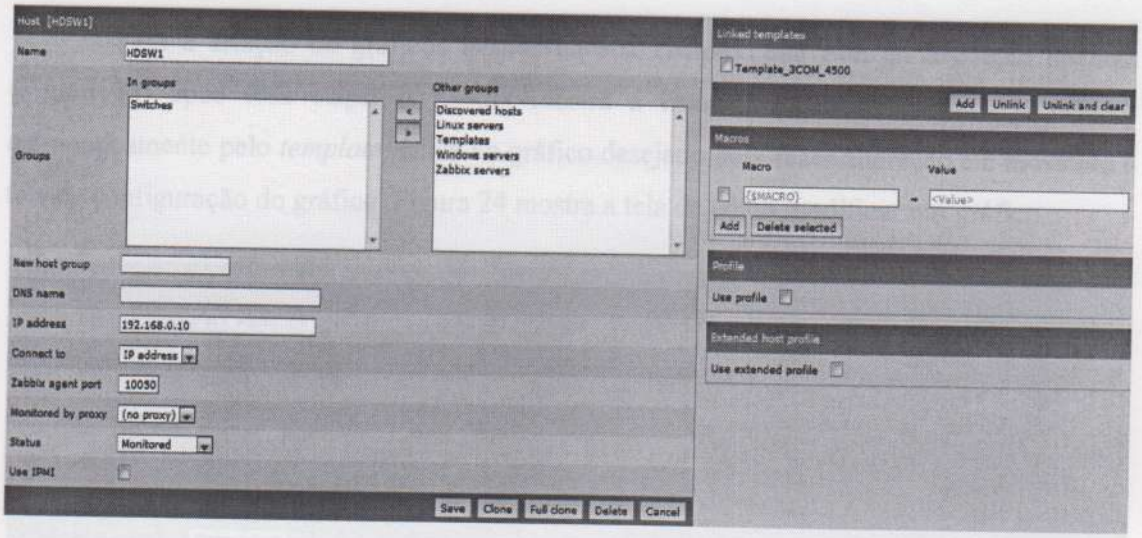


Figura 22: Configuração de um Host

O nome HDSW1, é a identificação do host, neste caso o switch de distribuição 1 da rede de homologação. O grupo é utilizado para facilitar a organização. O switch foi colocado dentro do grupo switches. O IP é o endereço que o host está configurado e o *Template* é um modelo de monitoramento pré-existente, o *Template* já vem configurado com vários triggers e gráficos personalizados em relação ao modelo de switch usado o 3com 4500.

Após o preenchimento dos atributos, clica em save para salvar as alterações feitas, agora o host já pode ser visualizado como monitorado. A figura 23 mostra o host sendo monitorado.

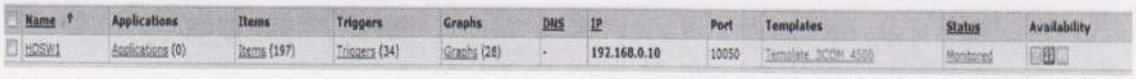


Figura 233: Host monitorado

Em cada coluna mostra as informações do host, como nome, aplicações a serem monitoradas, os itens monitorados, quantidade de triggers que geram as notificações e alarmes, a quantidade de gráficos que podem ser gerados através dos itens que estão sendo monitorados, em seguida informações sobre o DNS, endereço IP, porta e *templates* utilizados, o status do host que está sendo monitorado nesse momento e o método de monitoramento SNMP, mas também podemos monitorar o host através dos agentes Zabbix e ou IPMI.

3.6.9.2 Criação de Gráficos

Para a criação de gráficos iremos na aba *Graphs*, que está na discrição do host (Figura 23) após essa etapa, o Zabbix mostra a lista de todos os gráficos já criados automaticamente pelo *template*. Clica no gráfico desejado para fazer alteração e é mostrado a tela de configuração do gráfico. Figura 24 mostra a tela de como modificar um gráfico.

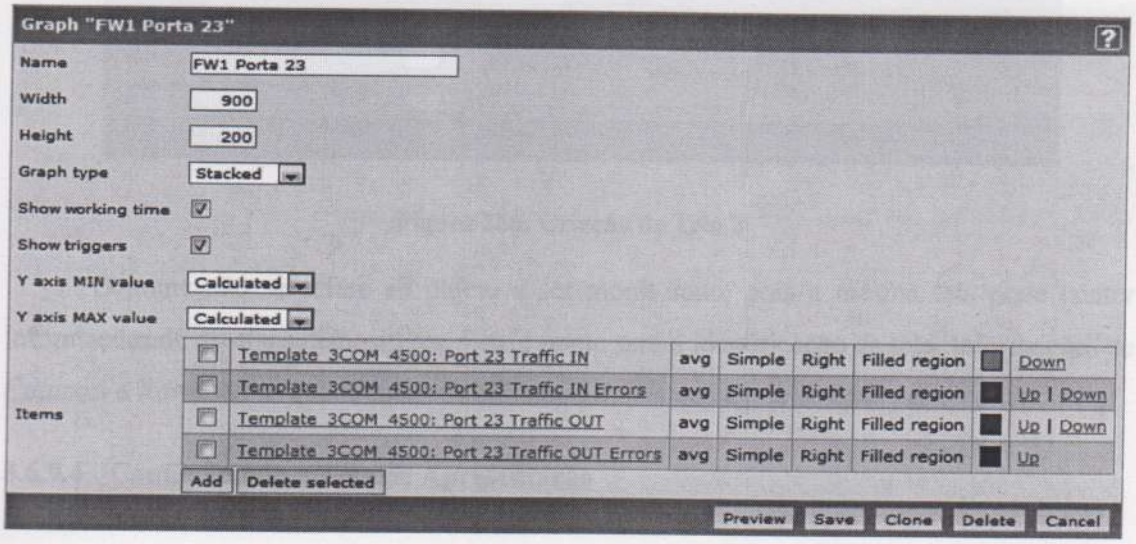


Figura 244: Modificação de gráfico

Aqui serão feitas as alterações desejadas, que neste caso é apenas a modificação do nome do gráfico, de "*Port 23 Traffic*" para "FW1 Porta 23", simbolizando que a porta 23 do switch é referente ao FWE1. Clicando em *preview* uma visualização do gráfico será mostrada

3.6.9.3 Configurando as Telas

As telas de apresentação são chamadas pelo Zabbix de *Screens*, ajudando a visualizar facilmente os dados que estão sendo recebidos a cada momento. Podendo fazer isso em formato de gráficos, textos, sumários, entre outros.

Para criar uma tela, é necessário acessar o caminho a seguir: *Configuration => Screens => Create Screen*. As Figuras 25 e 26 mostram o passo a passo das criações das telas.

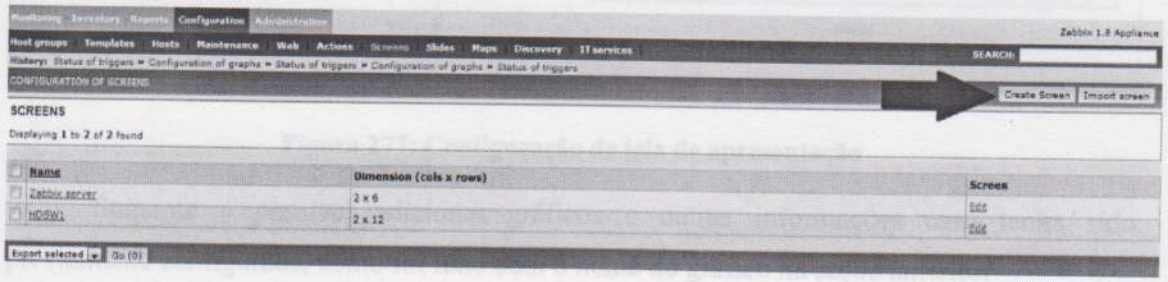


Figura 255: Criação de Tela 1

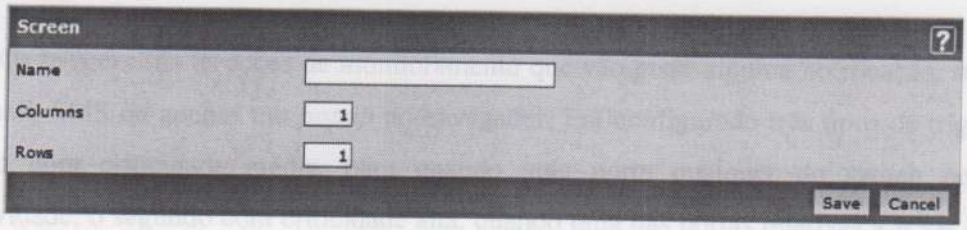


Figura 266: Criação de Tela 2

O nome não se refere ao objeto a ser monitorado, pois a mesma tela pode conter informações de diversos dispositivos. Este é nome será a identificação da tela. Informações de *Columns* e *Rows* são as quantidades de colunas e linhas que a tela desta *Screen* vai ter.

3.6.9.4 Configurando a Tela de Apresentação

Para configurar a tela de apresentação, deve-se clicar no nome da tela que deseja fazer a configuração e uma tabela irá aparecer. Cada célula irá conter um link *Change*, onde podem ser adicionadas informações.

Foi adicionado em uma célula da coluna o gráfico do tráfego de uma porta configurada com o *linkaggregation* do switch, e na outra célula um pequeno mapa interativo da rede, conforme a Figura 27.

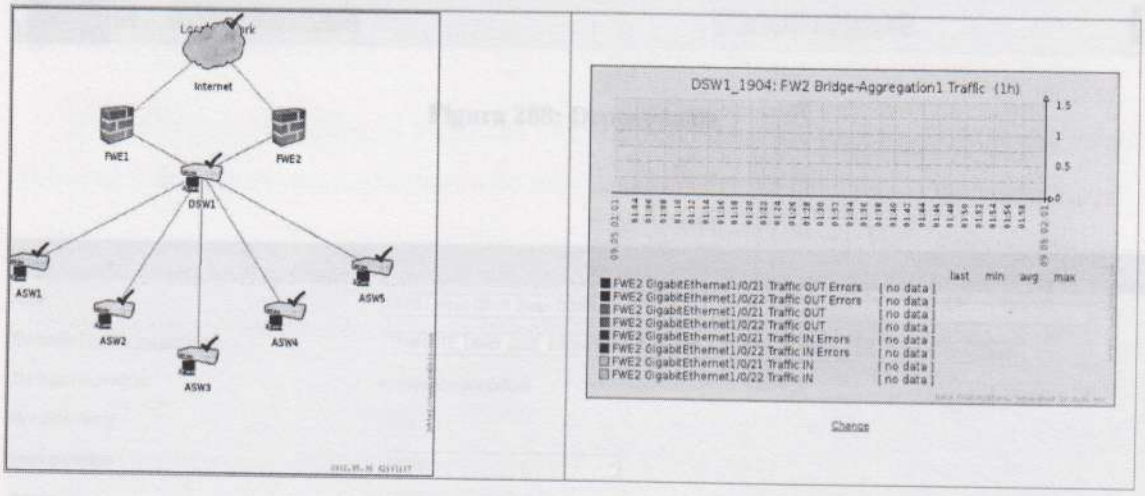


Figura 277: Configuração de tela de apresentação

Somente é possível adicionar gráficos e outras informações caso tenha sido previamente configurada, como foi feito com o nome do gráfico na seção anterior.

3.6.9.5 Definindo *Triggers*

Os *triggers* são as ações de monitoramento que vão gerar alguma notificação, seja ela um e-mail, SMS ou apenas um *popup* no navegador. Foi configurado três tipos de trigger, o primeiro com criticidade média, para quando uma porta qualquer do switch perca a conectividade; o segundo com criticidade alta, quando uma das portas relativas a ASW caia e o terceiro e último com criticidade Desastre caso de duas portas relativas ao mesmo ASW caiam ao mesmo tempo.

O primeiro tipo de trigger já vem configurada pelo *template* utilizado, a única alteração foi o nome, que é feito da mesma forma da mudança de nome do gráfico.

O segundo tipo de trigger de criticidade desastre foi feita apenas a modificação do nome, como no procedimento anterior e alteração da criticidade e colocando o *trigger* relativo à dois itens, como mostra as Figuras 28 e 29.

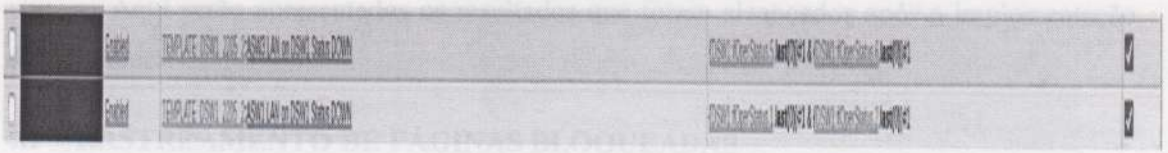


Figura 288: Dependência

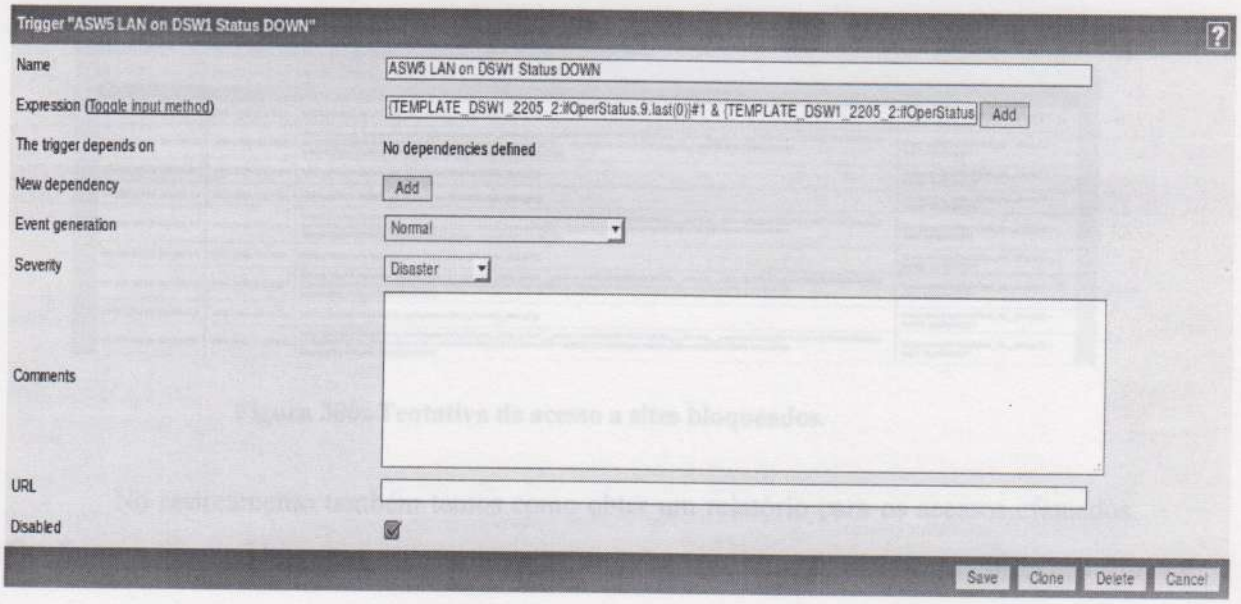


Figura 29: Criticidade desastre

4 RESULTADOS ALCANÇADOS

Aqui serão apresentados os resultados que foram alcançados após a implementação da nova rede.

4.1 RASTREAMENTO DE PÁGINAS BLOQUEADAS

Na Figura 30, podemos visualizar as tentativas de acesso feito as páginas que foram bloqueadas de acordo com a solicitação do setor de coordenação pedagógica do Senac.

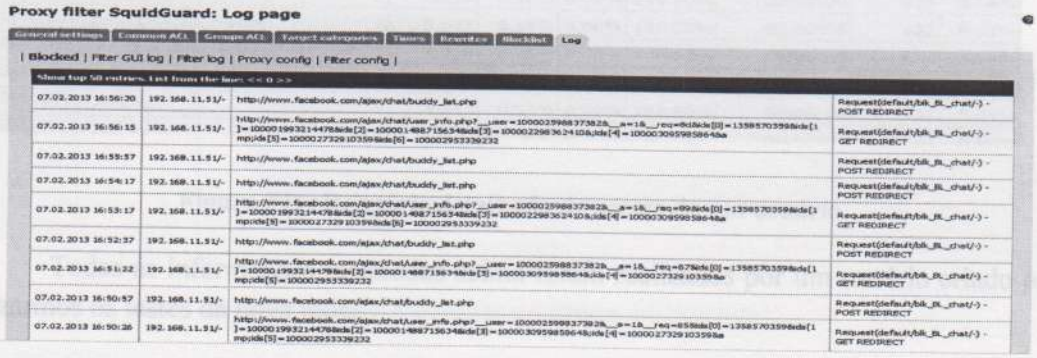


Figura 300: Tentativa de acesso a sites bloqueados.

No rastreamento também temos como obter um relatório para os acessos efetuados. Conforme a Figura 31.

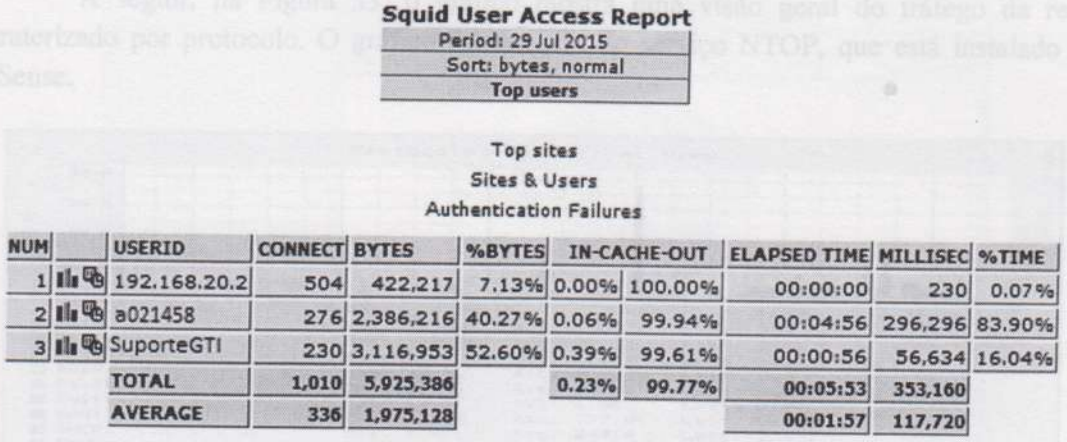


Figura 31: Relatório de acesso

Sendo necessário podemos ter acesso ao um relatório detalhado de todos os acessos de um determinado usuário. De acordo com a Figura 32.

Squid User Access Report
Period: 29 Jul 2015
User: francisco
Sort: bytes, normal
User report

ACCESSED SITE	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILLISEC	%TIME
click.uol.com.br	1	611	0.03%	0.00%	100.00%	00:00:00	69	0.02%
n.comentarios.uol.com.br	2	791	0.03%	0.00%	100.00%	00:00:00	134	0.05%
b.scorecardresearch.com	2	888	0.04%	0.00%	100.00%	00:00:00	162	0.05%
p.twitter.com	2	1,080	0.05%	0.00%	100.00%	00:00:00	301	0.10%
adclient-uol.ip.uol.com.br	1	1,652	0.07%	0.00%	100.00%	00:00:03	3,292	1.11%
d.i.uol.com.br	3	1,677	0.07%	0.00%	100.00%	00:00:07	7,052	2.38%
metrics.uol.com.br	2	1,940	0.08%	0.00%	100.00%	00:00:00	855	0.29%
cdn.api.twitter.com	2	2,084	0.09%	0.00%	100.00%	00:00:00	324	0.11%
n.i.uol.com.br	1	2,758	0.12%	0.00%	100.00%	00:00:00	109	0.04%
ia.rapmotion.com	1	2,818	0.12%	0.00%	100.00%	00:00:00	415	0.14%
view.comentarios.uol.com.br	2	3,047	0.13%	0.00%	100.00%	00:00:00	687	0.23%
ssl.gstatic.com:443	1	3,069	0.13%	0.00%	100.00%	00:00:00	674	0.23%
search.twitter.com	1	3,599	0.15%	0.00%	100.00%	00:00:00	354	0.12%
ca.i.uol.com.br	1	4,119	0.17%	0.00%	100.00%	00:00:00	121	0.04%
[illegible]	1	6,089	0.26%	0.00%	100.00%	00:00:01	1,747	0.59%

Figura 322: Relatório detalhado de acesso de um usuário

Todas as informações mostradas acima foram realizadas por um usuário criado para realizarmos os testes da nova rede.

4.2 TRÁFEGO DA REDE

Temos algumas ferramentas que são utilizadas para o gerenciamento e controle da rede, para facilitar o diagnóstico de possíveis falhas de segurança, além do acompanhamento do desempenho da rede.

A seguir, na Figura 33, o gráfico mostra uma visão geral do tráfego da rede, caraterizado por protocolo. O gráfico foi retirado do serviço NTOP, que está instalado no pfSense.

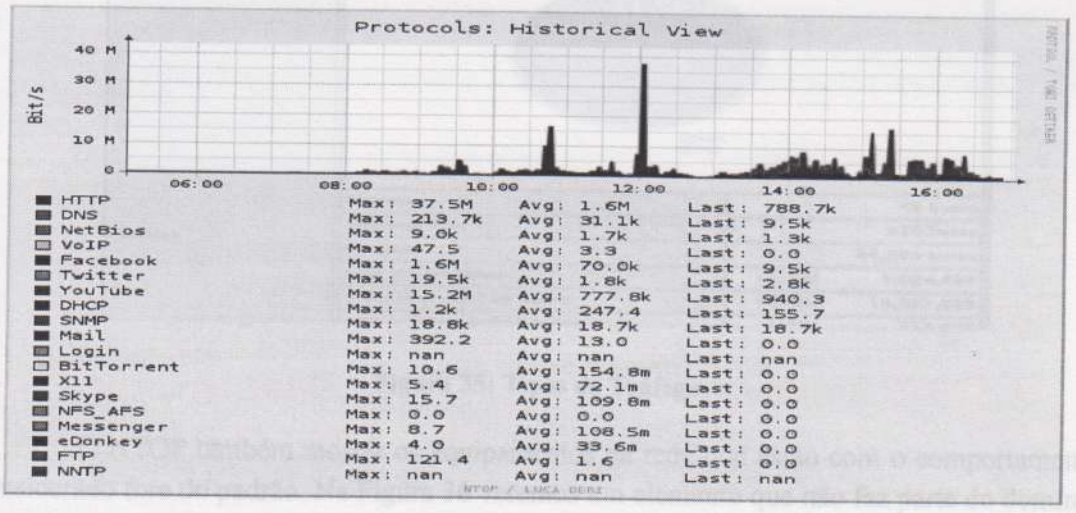


Figura 333: Visão geral do trafego de rede

O tráfego dos sites Facebook (1.6Mpbs) e YouTube (15.2Mpbs), correspondem a uma grande parcela do trafego total da rede, por este motivo foi solicitado pelo setor de TI o bloqueio dos mesmos.

Os dois sites mencionados correspondem a 17% da utilização total da rede. O consumo total da banda do YouTube de acordo com a Figura 34 mostra que ultrapassa 4gb no dia que foi realizado o monitoramento.

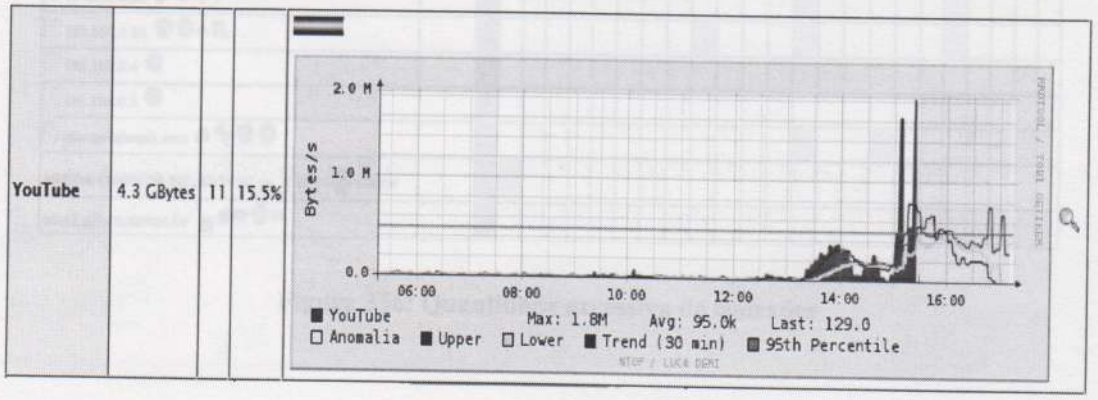


Figura 344: Consumo de banda do YouTube

O tipo de tráfego, mostrado na Figura 35, a importância da segmentação em VLANs, o tráfego de broadcast chega a 7%.

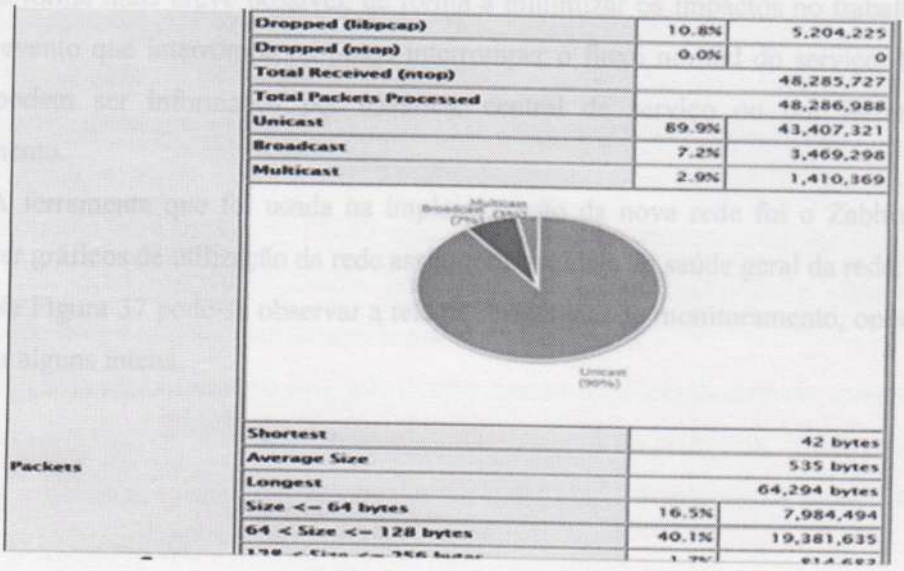


Figura 35: Tipos de Tráfego

O NTOP também mostra os equipamentos na rede que estão com o comportamento considerado fora do padrão. Na Figura 36 veremos um elemento que não faz parte do domínio que está com um excesso de conexões abertas para endereço remotos.

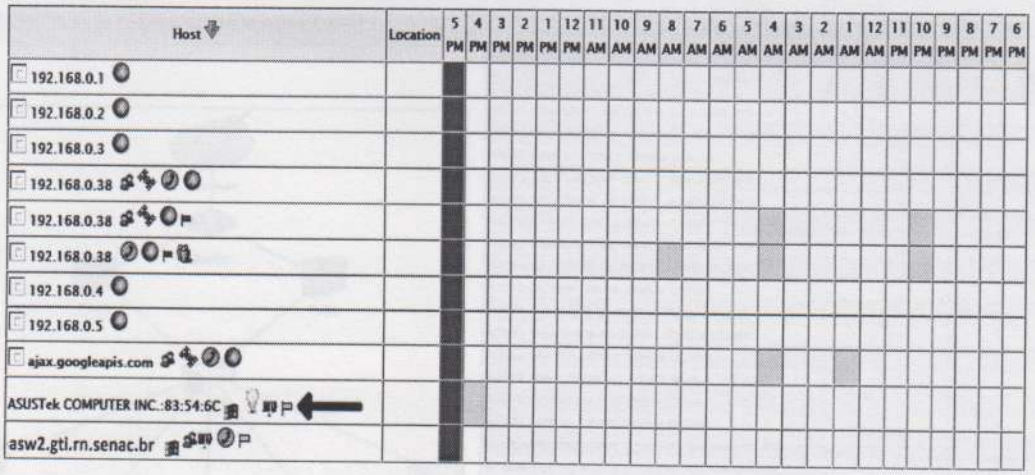


Figura 356: Quantidade excessiva de conexões

4.3 GERENCIAMENTO DE INCIDENTES COM ZABBIX

O gerenciamento de incidentes tem como objetivo a restaurar a operação normal do serviço da forma mais breve possível, de forma a minimizar os impactos no trabalho. Inclui qualquer evento que interrompa ou possa interromper o fluxo normal do serviço. Esses tais eventos podem ser informados por usuários, central de serviço ou por ferramenta de gerenciamento.

A ferramenta que foi usada na implementação da nova rede foi o Zabbix, ele vai permitir ver gráficos de utilização da rede assim ter uma ideia da saúde geral da rede.

Na Figura 37 pode-se observar a tela de ferramenta de monitoramento, onde podem-se destacar alguns intens.

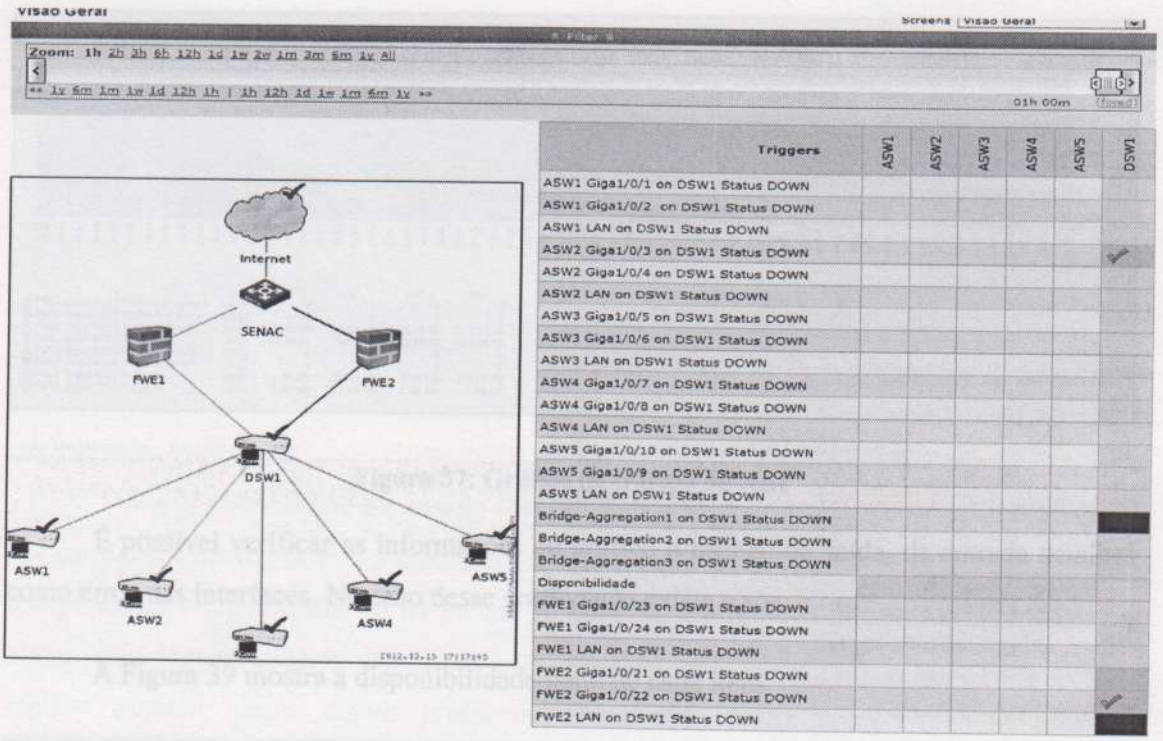


Figura 36: Visão Geral do monitoramento pelo Zabbix

A Figura 37 mostra a esquerda um pequeno mapa descritivo da rede, em que é possível localizar facilmente em que ponto está a falha. Uma linha verde entre os dispositivos mostra que a conexão está com seu funcionamento normal.

A linha amarela indica que a conexão entre o ASW2 e o DSW1 não está disponível, como o sistema conta com redundância, a conectividade ainda está estabelecida.

A linha vermelha que conecta o FWE2 a SENAC e ao DSW1, mostra que os links redundantes estão inoperantes. O FWE2 está desligado para mostrar todas as situações que podemos identificar usando o Zabbix para gerenciar a rede. Devido a redundância, a conectividade com a internet está garantida por meio do FWE1.

Também na imagem no seu lado direito mostra uma tabela com um resumo do que está acontecendo com os switches. Facilitando a localização do problema. Vemos que a porta 3 do DSW1 está sem conectividade e por isso a linha amarela indica que a conexão com o ASW1E está indisponível.

Já na conexão do FWE2, que está desligado, a informação é de que as portas 21 e 22 do DSW1 estão desligadas.

Na Figura 38 mostra informação do tráfego que está passando pelo DSW1 nas portas referentes ao FWE1, o gateway com a internet.

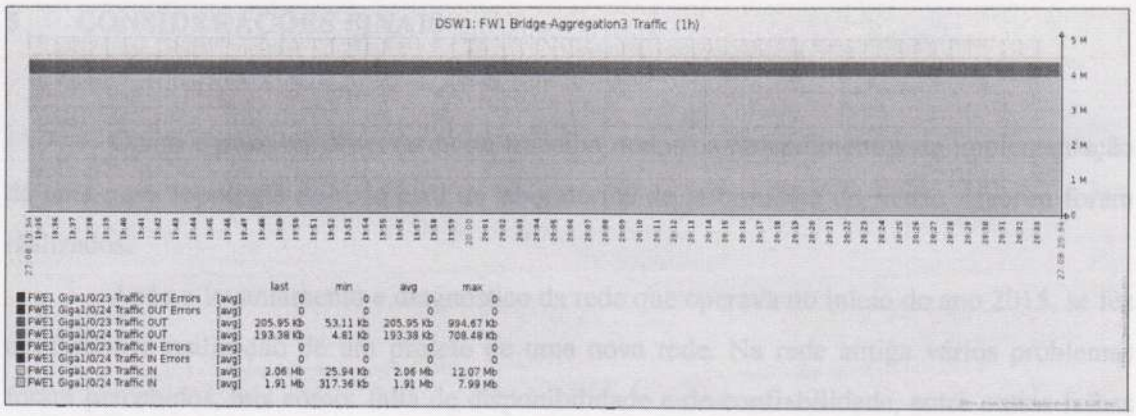
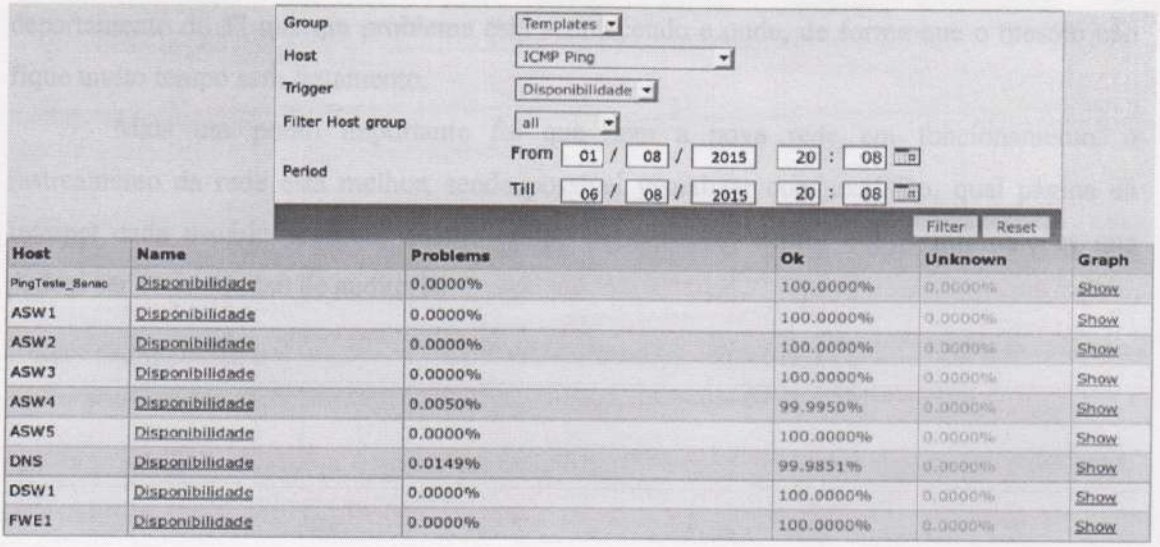


Figura 37: Gráfico de tráfego de rede

É possível verificar as informações do gráfico o tráfego de saída, de entrada detalhes como erros nas interfaces. No caso desse gráfico não existe erros.

A Figura 39 mostra a disponibilidade geral de cada item.



Host	Name	Problems	Ok	Unknown	Graph
PingTeste_Senac	Disponibilidade	0.0000%	100.0000%	0.0000%	Show
ASW1	Disponibilidade	0.0000%	100.0000%	0.0000%	Show
ASW2	Disponibilidade	0.0000%	100.0000%	0.0000%	Show
ASW3	Disponibilidade	0.0000%	100.0000%	0.0000%	Show
ASW4	Disponibilidade	0.0050%	99.9950%	0.0000%	Show
ASW5	Disponibilidade	0.0000%	100.0000%	0.0000%	Show
DNS	Disponibilidade	0.0149%	99.9851%	0.0000%	Show
DSW1	Disponibilidade	0.0000%	100.0000%	0.0000%	Show
FWE1	Disponibilidade	0.0000%	100.0000%	0.0000%	Show

Figura 39: Relatório geral de disponibilidade de elementos

A imagem mostra uma disponibilidade de aproximadamente 98,15%, abaixo 0,85% do definido como meta.

5 CONSIDERAÇÕES FINAIS

Como é possível observar neste trabalho, todos os procedimentos da implementação de uma nova topologia de rede para os laboratórios de informática do Senac Alecrim foram realizados.

Após o levantamento e diagnostico da rede que operava no início do ano 2015, se fez necessário a realização de um projeto de uma nova rede. Na rede antiga vários problemas foram percebidos, tais como: falta de disponibilidade e de confiabilidade, entre outras falhas encontradas.

Com o desenvolver do projeto foram notados alguns resultados importantes, como, por exemplo, a estabilidade e o gerenciamento da rede. Neste projeto a rede se mostrou mais independente e segmentada, de forma que as ações tomadas pelos usuários ou por falha em algum dispositivo, somente afetam uma determinada sala e não mais a rede toda. Assim, mesmo quando surgir algum problema, ferramentas estão prontas para alertar ao departamento de TI que um problema está acontecendo e onde, de forma que o mesmo não fique muito tempo sem tratamento.

Mais um ponto importante foi que com a nova rede em funcionamento, o rastreamento da rede está melhor, sendo possível visualizar com exatidão, qual página da Internet cada usuário acessou, quanto tempo permaneceu, dentre outras informações que podem ser úteis no caso de auditoria.

REFERÊNCIAS BIBLIOGRÁFICAS

Behrouz A. Forouzan. **Comunicação de dados e Redes de Computadores**. Bookman, 2006.

Douglas R. Mendes. **Redes de computadores teoria e prática**. Editora Novatec, 2007.

Edgar Jambour. **VLANs Ethernet**. Disponível em: <http://eureka.pucpr.br/repositorio/download.php/codLink=2068696>. Acesso em: 18 julho, 2015.

José Mauricio Santos Pinheiro. **Gerenciamento de rede de computadores**. Disponível em: <http://www.projetoderedes.com.br/artigo_gerenciamento_de_redes_de_computadores.PHP> . Acesso em: Junho, 2015.

Mario A. R. Dantas. **Computação distribuída de alto desempenho.** Axecel Books, 2005.

Mario A. R. Dantas. **Tecnologia de Redes de Comunicação e Computadores**. Axecel Books, 2002.

Mark Grennan. **Firewall and Proxy server howto**. Disponível em: <http://tldp.org/HOWTO/Firewall-HOWTO.html>. Acesso em: 23 julho, 2015.

Michelle D. Leonbardt. **Doroty: um chatterbot para treinamento de profissionais atuantes no gerenciamento de rede de computadores**. 2005

Odair Soares Barros. **Segurança de redes locais com implementação de VLANs – O caso da Universidade Jean Piaget de Cabo Verde**. Universidade Jean Piaget de Cabo Verde, 2009

Paulo Sergio Nicolleti Jaques Phillipe Sauvé, Raquel Vigolino Lopes. **Melhores práticas para gerência de rede de computadores.** Editora Campus, 2003

pfSense. **pfSense Features**. Disponível em: <http://www.pfsense.org/index.php>. Acesso em: julho, 2015

Shalla Secure Services KG, **Squidguard – site oficial**. Disponivel em: <http://www.squidguard.org> Acesso em: julho, 2015.

Simion Admans et al. **ITIL V3 foundation handbook**. Stationery Office, 2009.