
**ANTONIO MENEGHETTI FACULDADE - AMF**

**CURSO DE SISTEMAS DE INFORMAÇÃO**

**JEFERSON MANFIO**

# IMPLANTAÇÃO DE UMA INFRAESTRUTURA DE SEGURANÇA DA INFORMAÇÃO UTILIZANDO UTM FIREWALL

**RESTINGA SÊCA/RS**

**2016**

## Agradecimentos

Agradeço primeiramente a Deus por ter me proporcionado perseverança para concluir mais esta etapa da vida, a todos os amigos e colegas que me acompanharam nessa jornada acadêmica, onde muitas dificuldades foram enfrentadas, mas juntos conseguimos superar todas elas.

Obrigado a meus pais que sempre me incentivaram, a Dieli que esteve comigo sempre e também ao amigo José Luiz que em muito contribuiu para meu aprendizado e minha formação, tanto acadêmica quanto profissional. Também gostaria de agradecer a Prof. Ana e o Prof. Leonardo que me ajudaram a chegar nessa reta final do curso de Sistemas de Informação.

FACULDADE ANTONIO MENEGHETTI

Jeferson Manfio

# IMPLANTAÇÃO DE UMA INFRAESTRUTURA DE SEGURANÇA DA INFORMAÇÃO UTILIZANDO UTM FIREWALL

Trabalho de Conclusão de Curso-Monografia, apresentado como requisito parcial para a obtenção do grau de Bacharel em Sistemas de Informação, Curso de Graduação em Sistemas de Informação, Faculdade Antonio Meneghetti-AMF.

Orientador: Prof. Ms. Leonardo Guedes da Luz Martins

---

Prof. Ms. Leonardo Guedes da Luz Martins

Orientador do Trabalho de Conclusão de Curso

Antonio Meneghetti Faculdade

---

Profª Esp. José Luiz Rodrigues Filho

Membro da Banca Examinadora

Antonio Meneghetti Faculdade

---

Profª Ms. Fábio Sarturi Prass

Membro da Banca Examinadora

Antonio Meneghetti Faculdade

**Restinga Sêca, RS, 02 de julho de 2016**

# RESUMO

MANFIO, Jeferson. **Implantação de uma Infraestrutura de Segurança da Informação Utilizando UTM Firewall.** 2016. 38 páginas. Trabalho de Conclusão apresentado ao curso de Sistemas de Informação como requisito parcial para obtenção do título de Bacharel. Recanto Maestro-Restinga Seca/RS, 2016.

Essa pesquisa trata de demonstrar como é feita a implantação de um UTM *Firewall* em uma Infraestrutura de Segurança da Informação. A mesma tem o intuito de esclarecer como funciona a ferramenta e como utilizar seus recursos básicos, a sim de mostrar que tem-se soluções relativamente novas no mercado, a um custo acessível para a maioria dos ambientes de médio a grande porte.

**Palavras-chave**: Segurança, Redes, *UTM Firewall.*

# ABSTRACT

MANFIO, Jeferson. **Implantação de uma Infraestrutura de Segurança da Informação Utilizando UTM Firewall.** 2016. 38 pages. Completion of Work presented to the course of Systems Information as a partial requisit for Bachelor Title procurement. Recanto Maestro-Restinga Seca/RS, 2016.

This research is to demonstrate how is the implementation of a UTM Firewall in a Security Infrastructure Information. The same is intended to clarify how the tool and how to use its basic features, but to show that we have relatively new solutions on the market, at an affordable cost for most medium to large environments.

**Keywords**: Security, Networks, UTM Firewall.

**Termos**

UTM - *Unified Threat Management* (tratamento unificado de ameaças)
TI – Tecnologia da Informação
*Proxy* – ferramenta utilizada no controle de acesso à WEB
*Spyware* – software espião, geralmente com o objetivo de roubar dados
*Malware* – software mal-intencionado, causa danos ao computador
VPN – *Virtual Private Network* (rede virtual privada)
IPS – *Intrusion Prevention System* (sistemas de prevenção de intrusos)
*Phishing* – do inglês pesca - são tentativas de roubo de dados pessoais, comumente utilizados em golpes financeiros.
DMZ - *Demilitarized Zone* (zona desmilitarizada)
LAN – *Local Area Network* (rede local/interna)
Trends: ferramenta on-line do Google que gera gráficos dos termos mais pesquisados.
WAN – *wide area network* (grande rede)
LAN – *local area network* (rede interna)
*Whatsapp* – aplicativo móvel para troca de mensagens de texto e arquivos multimídia.

## Lista de figuras

# Sumário

## 1. Introdução

Com o advento da internet e seu crescimento exponencial, tem-se a liberdade de acesso a qualquer conteúdo em praticamente qualquer lugar. A internet é uma ferramenta presente na nossa rotina, que certamente traz muitos benefícios na execução dos trabalhos, além de também poder ser utilizada como ferramenta de negócios ou meio de entretenimento para as pessoas.

O conteúdo que trafega por ela ultrapassa as barreiras geográficas e por vezes não há como mantermos o controle sobre o que as pessoas estão acessando. Assim, essa ferramenta precisa ter seus acessos restritos, ou seja, faz-se necessário um controle que não deve ser compreendido como arbitrariedade nem restrição de acesso, mas sim como forma de preservação de segurança da informação do ambiente.

Segurança certamente é um dos assuntos mais importantes quando tratamos de rede de computadores, pois ninguém gostaria de ter seus dados acessados ou seu trabalho destruído por uma pessoa mal intencionada, por isso é tão importante manter o controle total de uma infraestrutura, pelo menos no que diz respeito a parte virtual do ambiente.

Este projeto visa elucidar a implantação de uma ferramenta *UTM Firewall* em um ambiente público, procurando fazer com que as pessoas entendam melhor o que é segurança da informação. Também tem por objetivo esclarecer o funcionamento desta ferramenta e demonstrar os benefícios proporcionados ao gerenciamento do ambiente. Tudo isso sendo feito em uma plataforma unificada, voltada para a proteção das informações em um ambiente com um número significativo de usuários no cumprimento de suas tarefas.

### 1.1. Problema de pesquisa

Diante da maior complexidade das ameaças que os usuários estão expostos na internet, cada vez mais as empresas preocupam-se com a segurança da informação. Com isso, surgiu a necessidade de novas ferramentas para garantir a segurança e controle do que trafega pela rede, assegurando uma maior produtividade na organização, atingindo de forma direta quem trabalha utilizando o computador e demais dispositivos conectados à uma rede durante sua jornada de expediente.

Empresas e usuários cada vez mais estão expostos a riscos na utilização de seus computadores e dispositivos no acesso à internet. Este projeto tem por objetivo esclarecer como funciona essa nova geração de *firewalls* com gerenciamento unificado, onde temos todo gerenciamento necessário em uma só ferramenta, tornando o controle e configuração mais fácil, logo, menos tempo para encontrar e corrigir possíveis falhas e/ou ameaças.

O problema da pesquisa desse projeto, baseou-se na necessidade de atender uma infraestrutura de tecnologia da informação de um órgão público, em todos os setores, de modo

que todo gerenciamento e configurações de segurança fossem feitos em somente uma interface.

## 1.2. Justificativa

As empresas preocupam-se mais a cada dia quando o assunto é tecnologia da informação e estão dispostas a investir nela. Ainda mais levando-se em conta o cenário atual, em que cada vez mais tentamos tirar vantagem competitiva com o uso de softwares integrados, profissionais da área técnica e colaboradores capacitados para operá-los de forma otimizada. Ferramentas que nos auxiliam na tomada de decisão são essenciais, sejam elas softwares, hardwares ou soluções integradas.

Com isso, o uso de uma ferramenta de fácil manipulação, que não necessite de constantes alterações em suas configurações, com hardware próprio (desenvolvido pelo fabricante), que disponibilize relatórios de acesso e de consumo de banda tornou-se o objeto de pesquisa abordado.

O intuito deste trabalho, é facilitar o entendimento de como essa ferramenta de segurança unificada funciona, quais os benefícios trazidos, como são aplicados filtros, bloqueios, regras para acesso a aplicações web, bem como mostrar o resultado final por meio de gráficos que possam comprovar seus benefícios.

## 1.3. Objetivos

### 1.3.1. Objetivo Geral

Mostrar como uma infraestrutura de TI dentro de um ambiente corporativo pode ser melhorada com o uso de uma ferramenta UTM. Demonstrar os resultados obtidos e comprovar sua eficácia, esclarecer como uma rede pode ser melhorada com a utilização dos recursos aplicados de forma consciente.

A pesquisa pretende mostrar que com apenas uma ferramenta unificada é possível fazer o mesmo trabalho que antes era feito por várias para controlar o acesso de conteúdo web (websites e aplicações específicas) bem como a segurança da rede.

### 1.3.2. Objetivos Específicos

Os objetivos específicos deste projeto são:

- Mostrar o levantamento de requisitos para a implantação de um UTM Firewall;
- Elucidar como funcionam as regras de *firewall*;

- Mostrar o conteúdo web mais acessado baseado nos dados coletados por meio de gráficos da própria ferramenta.

### 1.4. Estrutura do Trabalho

Esse trabalho foi desenvolvido com seis capítulos, onde o primeiro é uma introdução com o problema de pesquisa, seguido de uma justificativa, objetivo geral e específico.

No capítulo dois tem-se um referencial teórico onde são descritos conceitos, de *firewall,* redes, segurança, bem como os recursos de uma ferramenta UTM.

No capítulo três, dentro da metodologia procurou-se fazer aplicar os recursos do referencial teórico. Temos também o levantamento de requisitos, estudo de caso e uma breve explicação a respeito da ferramenta UTM.

No capítulo quatro, pode ser vista a implantação do UTM na Infraestrutura de Segurança.

No quinto capítulo é evidenciado o resultado obtido com a aplicação prática do objeto de pesquisa demonstrado por alguns gráficos gerados dentro da ferramenta.

E por fim, no sexto capítulo temos algumas considerações finais obtidas ao longo da pesquisa e o depoimento de alguns colaboradores pertencentes ao ambiente.

## 2. Referencial Teórico

Um UTM do inglês *(unified threat management)* – gerenciamento unificado de ameaças, é um firewall com soluções unificadas como o nome sugere, composto por sete camadas.

Segundo a empresa Microsoft (2014), Firewall pode ser um software ou hardware que constantemente verifica informações provenientes da internet ou de uma rede e as bloqueia ou permite que elas cheguem a um computador, dependendo das configurações do firewall. Um *firewall* pode ajudar a impedir que hackers ou softwares mal-intencionados obtenham acesso não autorizado em um computador por uma rede ou pela internet.

Já a empresa de *firewall* Fortinet (2014), diz que um UTM *Firewall* é uma tecnologia voltada para a segurança de rede, que tornou-se a principal solução para proteção corporativa nos últimos anos. A segurança UTM é a evolução do *firewall* tradicional, sendo assim uma solução de segurança mais robusta e completa.

Para a empresa Sophos (2014), UTM *Firewall* são definidas como *firewall* avançadas, possuem funcionalidades de prevenção de intrusos e controle de aplicações, os sistemas UTM também associam essas funcionalidades a outras tecnologias adicionais, como proteção de e-mail, filtro de URLs, poteção de rede *wireless*, VPNs (rede virtual privada).

Desta forma os benefícios obtidos através desta tecnologia são para se proteger de invasões, *malware*, ataques, controle e visualização em tempo real. Também fazem filtragem de conteúdo, *antispam*, antivírus e proteção contra invasões. (SONICWALL, 2014). Oferece ainda proteção abrangente contra ameaças, enquanto reduz despesas capitais e operacionais de empresas. Proporciona um ambiente seguro, oferecendo total controle no acompanhamento da atividade do usuário, melhorando assim a produtividade e atendendo às exigências de conformidade regulatória. (CYBEROAM, 2014).

As ameaças estão ficando cada vez mais sofisticadas. Uma combinação externa de ameaças como vírus, *spyware*, Cavalos de Tróia e *phishing* causam grandes transtornos a redes de empresas. A abordagem tradicional de empregar apenas *firewall* e antivírus não é mais o suficiente, com isso, as empresas precisam de soluções de segurança múltiplas para combater ameaças mistas. (CYBEROAM, 2014).

Com essa necessidade tem-se o UTM que é uma ferramenta que oferece solução abrangente para as organizações, que vão desde grandes empresas até filiais e pequenos escritórios. Possui recursos de segurança integrados em uma única plataforma baseada em identidade, tornando a segurança eficaz. (CYBEROAM, 2014).

Uma das maiores vantagens de usar-se UTM ao invés de ferramentas de segurança comuns é não ter que manipular vários softwares de segurança (*firewall*, *proxy*, VPN, antivírus, IPS) dentro de um mesmo computador. Fabricantes de UTM são empresas de TI que geralmente vendem o hardware em conjunto com o software.

Recursos proporcionados pelo uso de um UTM *Firewall*:

- Proteger as redes e usuários de downloads inesperados, vírus, *spyware* e outros *malwares*.
- Os administradores da rede podem monitorar o comportamento dos usuários na web de maneira precisa e individual a fim de identificar qualquer comportamento suspeito.
- Alta disponibilidade da rede, sem abrir mão da segurança e desempenho.
- OS relatórios de acesso ficam armazenados na ferramenta.

## 2.1. Sobre o *Firewall*

É basicamente o que há entre o computador e a internet. É um software capaz de gerenciar regras de entrada ou saída. As regras nele configuradas são as regras que podem permitir ou negar a entrada ou saída de protocolos, categorias de conteúdo, determinar quais operações de entrada ou saída podem ser executadas ou negar o acesso a endereços IP válidos ou inválidos.

Ele é uma solução voltada para segurança e normalmente baseia-se em software (na forma mais comum) ou hardware, na forma traduzida o termo "*firewall"* faz referência a uma "parede" usada para defesa, onde nela é possível efetuar o bloqueio de tráfego irrelevante, bem como permitir ou priorizar o tráfego útil para o ambiente.

Pode-se imaginar um *firewall* como sendo um porteiro na entrada de um condomínio residencial. Se você quiser entrar, deve identificar-se, ser convidado por alguém, obedecer determinadas condições de segurança e não trazer consigo nada que possa oferecer riscos. Do mesmo modo, ao deixar as dependências do local, não deve levar nada do ambiente a menos que tenha autorização do proprietário.

Nos *firewalls*, contamos com a tecnologia de filtro de pacotes de dados. Cada pacote de dados possui em seu cabeçalho algumas informações como de onde originou e para onde está indo (através do IP de origem e destino), qual tamanho o pacote possui e qual seu tipo de serviço. A partir desse momento o *firewall* analisa as informações desses pacotes, tomando a ação de permitir ou negar tanto a entrada quanto a saída deles, de acordo com o que foi configurado nas regras de *firewall*. É importante ressaltar que a transmissão dos dados em um *firewall* é feita com base no padrão TCP/IP.

A imagem abaixo pode nos ajudar a compreender como funciona um *firewall* em sua função mais simplificada, sem filtro de pacotes:

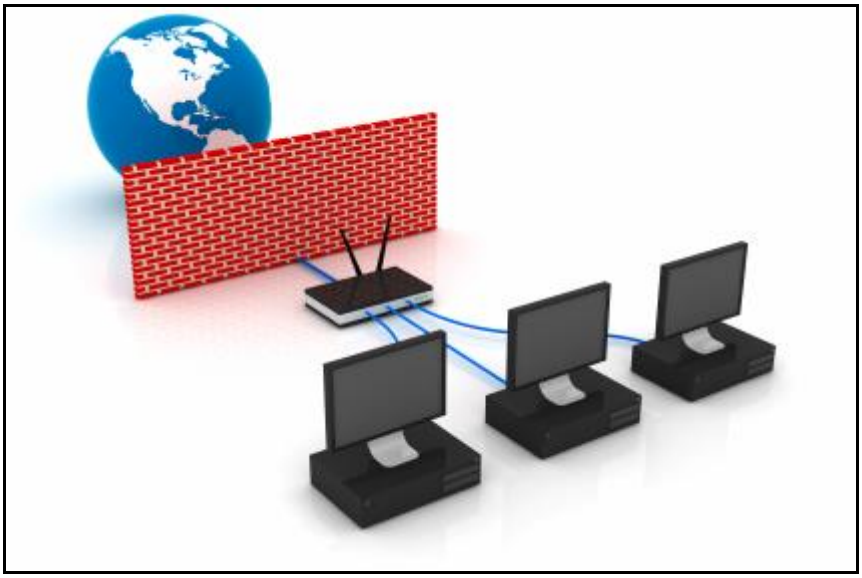


Figura 1- O funcionamento de um *Firewall* em uma rede
Fonte: http://www.ebrahma.com/wp-content/uploads/2015/04/Firewall-%E2%80%93-Basic-concepts.jpg

Quando fazemos referência a um *firewall* com filtro de pacotes, normalmente ele possui o recurso de *Proxy* (filtro web que será visto mais adiante). Este tipo de *firewall* intercepta toda comunicação que entra e sai da rede, ou seja, é uma intermediação entre a rede externa WAN e a rede interna LAN (veremos o que é WAN e LAN a seguir), de forma que

não seja permitida comunicação direta entre essas duas áreas. Baseado nisso, o mesmo toma a ação de negar ou permitir, de acordo com as regras configuradas.

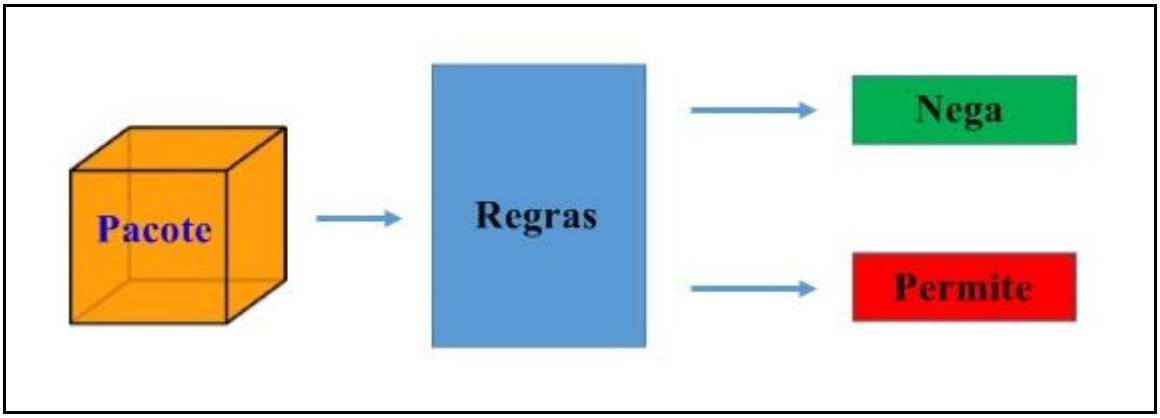



Figura 2 – Funcionamento de um *Firewall* com filtro de pacotes

No momento em que um *firewall* verifica toda informação que passa por ele (entra ou sai do computador para a rede), automaticamente fecha-se o cerco contra invasões. Ele fecha todas as portas de acesso que não são padrão dos sistemas operacionais, que são por onde os serviços comunicam-se. A partir desse ponto, somente esses computadores e portas autorizadas são os que podem ter comunicação. Na prática obviamente um *firewall* não bloqueia todas as portas de comunicação, pois assim um computador perderia a sua utilidade.

Nesse projeto de pesquisa trataremos de forma mais específica sobre o *firewall* de hardware com *appliance* que é o conceito de *UTM Firewall*. Também há o *firewall* que é instalado em cada computador por padrão, este, comumente é chamado de *firewall* pessoal. É muito importante esclarecer que o uso de um *firewall* não é garantia de proteção completa, sendo assim, a prevenção, uso de software antivírus e bom-senso no acesso à informação sempre são medidas bem-vindas quando abordamos o assunto segurança.

### 2.1.1. Redes e Endereço IP

Endereço de IP válido significa um endereço IP da grande internet, onde a empresa ou residência do usuário possui um IP somente para ela. Como ter um endereço IP “próprio” tem um custo adicional, pois o número de endereços IP não é infinito, normalmente os provedores ou operadoras de internet entregam o acesso web para os clientes através de um IP inválido.

Essa entrega só é possível através da criação de uma sub-rede. Assim, o IP válido normalmente é configurado em um servidor ou roteador e todos os demais computadores da sub-rede acessam a internet através dele, dessa forma em uma visão global da rede há somente um endereço IP válido e todos os demais dispositivos pertencentes à sub-rede conectam-se à grande rede através destes endereços IP válido.

Dessa forma devemos compreender o conceito de WAN e LAN, qual o significado dessas duas siglas e como elas funcionam, pois comumente são encontradas na tela de configuração de nossos modems, roteadores e pontos de acesso domésticos.

WAN *(wide area network)*: é uma rede que cobre uma área física maior, normalmente a internet chega por um cabo após o modem, antena ou roteador da operadora, ou provedor, por um cabo de rede que vai plugado na interface de rede WAN do *firewall*. Sendo assim, de forma simplificada podemos dizer que WAN é o que dá acesso à grande rede de internet que nos conecta com o mundo. Em links comerciais normalmente o fornecedor de internet entrega um IP válido através dessa rede, onde depois é feito o roteamento para a rede LAN.

LAN *(local area network)*: essa é a rede local de computadores e é também chamada de rede interna. Um exemplo de LAN é a rede de nossa casa ou escritório, onde em sua forma mais comum é a rede computadores restrita a somente um local físico. Uma rede sem fio de casa ou empresa também faz parte da rede LAN que possui uma faixa de IP restrita para uso interno.

Na figura 3 a seguir, pode ser visto o cenário de uma rede LAN, típico do ambiente que possui matriz e filiais que precisam estar interligadas por razões operacionais, que muitas vezes podem incluir a execução de serviços que funcionam em um mesmo servidor.

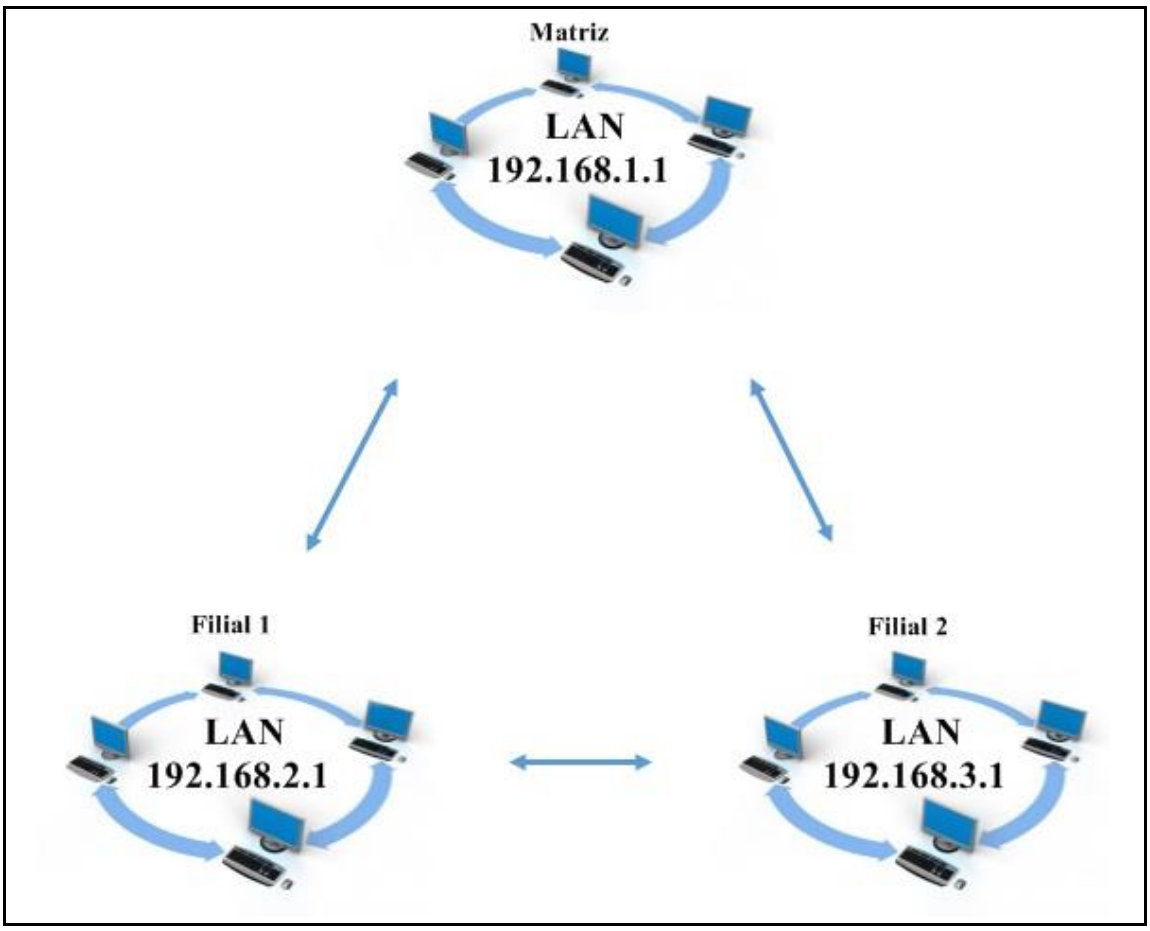



Figura 3 – Interligação pela rede LAN

Já a rede WAN é uma rede composta de vários “conjuntos” de redes LAN que podem estar em nosso bairro por exemplo. Este tipo de rede vai um pouco além das demais e consegue abranger uma área maior, por isso é chamada de rede de longa distância. Pode ser observado o esquema de uma rede WAN na figura 4 a seguir:

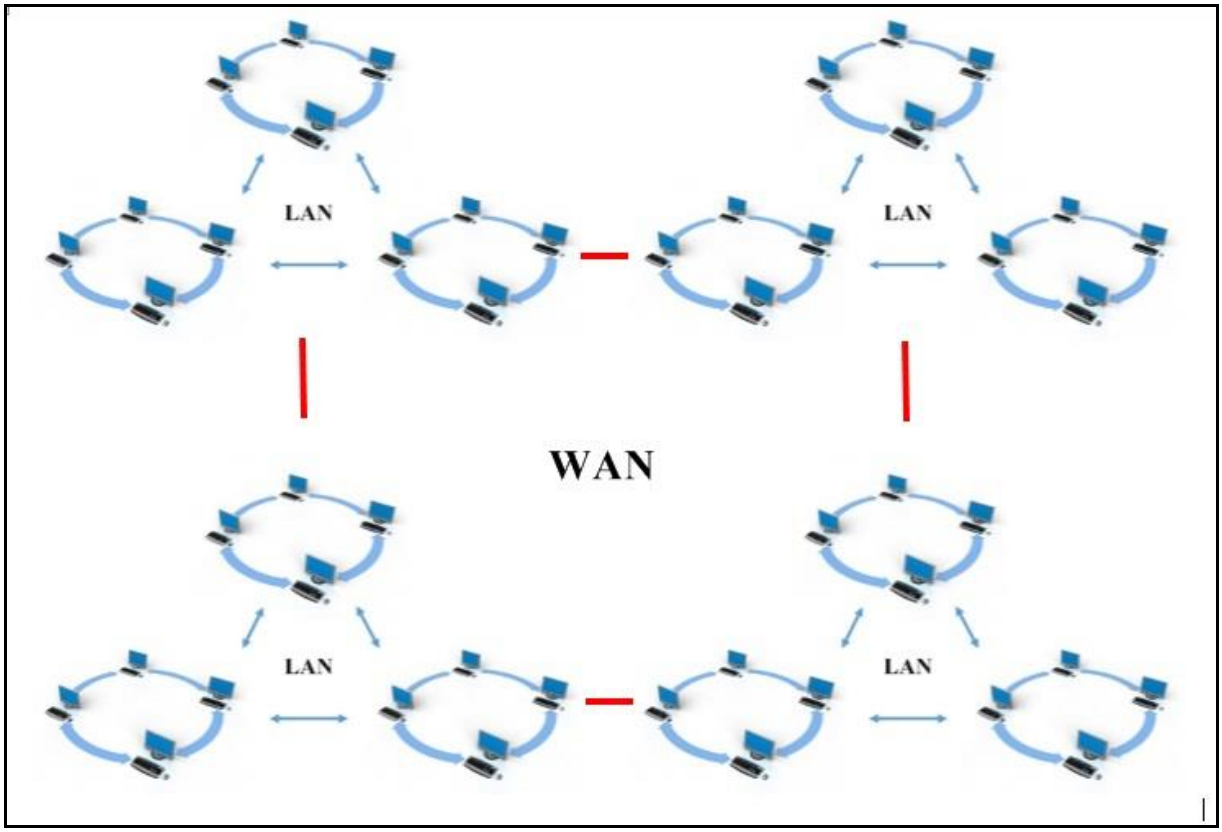



Figura 4 – Interligação pela rede WAN

DMZ: também conhecida como Zona Desmilitarizada. Fica localizada entre uma rede interna e uma rede externa (intranet e internet). Na forma ideal, é destinada aos servidores, assim é possível fazer com que o IP da rede externa seja redirecionado ao servidor da rede interna (que está na zona DMZ) para rodar os serviços web. A partir desse ponto, todos os demais computadores da rede (estes ficam na LAN) rodam sistemas, acessam à internet e fazem acesso aos servidores que ficam na DMZ para a execução dos sistemas de gestão.

## 2.2. Segurança

Quando falamos em segurança, inevitavelmente pensamos na internet, pois é ela que os ataques ocorrem com mais frequência, mas não é somente isso. A segurança também faz referência ao que envolve autorização para acessar os dados de uma rede, os quais normalmente são gerenciados pelos administradores de redes. As tecnologias de segurança de redes servem para proteger os computadores e seus sistemas do vazamento de informações confidenciais, ou utilização inapropriada destas, bem como evitar contaminações por vírus que nos expõem a vulnerabilidades.

Os principais conceitos de segurança da informação são: integridade, disponibilidade e confidencialidade.

Integridade: garante que o conteúdo da informação não seja alterado ou violado sem permissão. Perde-se a integridade quando a informação é alterada de forma indevida.

Disponibilidade: garante disponibilidade da informação quando desejado. Remete ao correto funcionamento da rede e sua eficácia, podendo garantir o correto funcionamento da mesma, dessa forma quando for necessário buscar essa informação ela estará disponível para ser imediatamente acessada.

Confidencialidade: garante que a informação seja acessada somente pelas pessoas que tem autorização. A forma principal de garantir controle no acesso à informação é pelo controle de acesso autenticado. A confidencialidade começa a partir do momento em que impedimos que pessoas não autorizadas tenham acesso ao conteúdo de uma mensagem ou que as informações sejam divulgadas de forma não permitida.

Graças a segurança, é possível monitorar e prevenir variados tipos de acesso indevido. Não utilizar o recurso de segurança pode ter um preço elevado e efeitos catastróficos, tais como: falhas de comunicação, interrupção dos serviços até mesmo parada total do ambiente até que seja tomada uma ação corretiva. Esta ação por sua vez, com certeza irá envolver segurança aplicada.

Dentre os problemas mais comuns encontrados na segurança de rede está o furto de dados, que é quando dados ou informações são obtidos pela interceptação do tráfego ou pela exploração de vulnerabilidade de acesso no computador. Em seguida, vem as infecções por vírus que muitas vezes contaminam a rede, gerando grandes transtornos para toda a infraestrutura do ambiente.

A segurança tem por objetivos:

- Controlar e identificar usuários do sistema, evitando que pessoas não autorizadas tenham acesso às informações. Assim, é prevenido o roubo ou utilização inadequada destas;
- Proteger contra ameaças internas e externas que podem representar riscos ao sistema da empresa, analisando processos e monitorando atividades estranhas, assim é possível tratar da forma mais apropriada;
- Garantir privacidade nas comunicações. Quando algum colaborador estiver viajando e precisar acessar o sistema da empresa, este acesso deve ser feito com a permissão do administrador, sem que haja comprometimento da segurança nem traga riscos ao ambiente.

### 2.2.1. Recursos de um UTM

Filtro de aplicações *(application filter):*

Um filtro de aplicação serve para que possamos “filtrar” todo tipo de aplicação web. É um método de permitir ou interromper o acesso à determinada categoria ou aplicação de forma coletiva (grupo de aplicativos) ou em específico (somente uma aplicação).

*Appliance:*

Uma *appliance* pode ser traduzida na forma mais genérica como “ferramenta”. Na informática, as *appliances* são máquinas (computadores) pré-configurados para executar um trabalho específico. Normalmente elas são voltadas para aplicações de automação, caixas registradoras ou de firewall.

Estas, podem ser montadas em um gabinete ou case específico, e o hardware deve ser robusto. Ao contrário do que pode parecer, nem sempre são dispositivos difíceis de construir. Pelo contrário, às vezes é um computador comum que foi montado em um gabinete diferente acoplado a um leitor de código de barras ou o que for necessário para executar suas tarefas. Um exemplo claro que a maioria conhece são os computadores de caixas dos grandes supermercados, estes são *appliances* (MORIMOTO E. CARLOS, 2005).

*Reports* (relatórios):

Relatórios são sempre importantes no momento da tomada de decisão, às vezes as empresas, por necessidade trocam de sistema simplesmente porque o utilizado não atendia a obtenção de resultados mostrados em relatórios. Afinal, nada melhor que tirar um relatório para demonstrar a eficiência de um trabalho ou ferramenta, comprovando que o trabalho desenvolvido está sendo feito da forma mais eficiente.

No próximo capítulo veremos como funcionam os relatórios de uma *appliance* de *firewall*, estes são gerados em forma de gráfico, de forma muito intuitiva, para que sejam compreendidos até mesmo por um usuário mais leigo.

Balanço de carga *(load balance):*

Uma capacidade muito interessante de um UTM é trabalhar com balanço de carga. Ela funciona da seguinte forma: é possível ter dois ou mais links de internet trabalhando em conjunto.

Cada um desses links no balanço de carga pode ter ou seu “peso” configurado, ou seja, o link de maior velocidade geralmente é configurado com um peso maior para ele. Na prática, isso quer dizer que quanto maior a carga configurada para determinado link, mais tráfego irá chegar na rede por ele.

Para compreender melhor, imaginemos o seguinte cenário: No momento em que esse link começa a ficar lento (no limite do tráfego fornecido pelo provedor) automaticamente os computadores na rede do *firewall*, passam a navegar pelo link alternativo, sem qualquer impacto na navegação web do usuário final. Ainda há a opção de fazer com que usuários ou computadores naveguem por um link específico. Exemplo: no departamento financeiro os computadores usam um link de 10Mbps e no RH usam o link de 1Mb.

## 3. Metodologia

Este trabalho foi desenvolvido através do estudo de caso de uma infraestrutura de TI. Surgiu a necessidade de um filtro de aplicações e conteúdo para aumentar a segurança da

informação, bem como a produtividade dos colaboradores. Na sequência, foi determinado qual equipamento deveria ser usado para dividir e gerenciar a rede de computadores.

### 3.1. Levantamento de requisitos

Dentre os requisitos para a escolha da ferramenta estiveram os seguintes:

- Facilidade de manipulação: que as configurações mais utilizadas, tais como o gerenciamento de regras de acesso ou bloqueios, pudessem ser feitos de forma ágil, até mesmo pelo usuário final.

- Escalabilidade: pensando um uma futura expansão no número de computadores, servidores ou aumento de usuários, a ferramenta deveria suportar essa exigência extra sem mais investimentos.

- Confiabilidade: por possuir hardware próprio não haveria preocupação com falhas físicas nem gastos com compras de peças para mantê-lo funcionando.

- Idioma: há uma limitação na ferramenta por parte do idioma, pois o mesmo é em inglês, porém é um idioma global, onde os termos técnicos são padrão como em outras ferramentas. Isso talvez seja um problema para quem não o domina, mas em contrapartida ele é muito intuitivo, um inglês intermediário ou até mesmo básico por parte do administrador deve ser suficiente para que possa compreender todos os recursos da ferramenta e utilizá-la de forma plena.

- *Proxy/web filter:* proporciona o controle de navegação. Podemos definir sites permitidos ou bloqueados, de forma individual para cada usuário ou grupos de usuários. O filtro web bloqueia desde um site individual até uma categoria inteira de sites. Exemplo: pode ser bloqueada a categoria de sites “rede sociais”. Dentro dessa categoria, por padrão já estão todos os sites que fazem referência a ela.

- Baseado em identidade: que a administração dos bloqueios e permissões não fossem efetuados apenas pelo IP do computador, mas por usuário e senha também. Assim torna-se mais fácil a visualização dos *logs* e relatórios. Esse controle através da criação de usuário e senha nos permite que sejam criados grupos de usuário e torna a manipulação das regras mais fácil, esse controle chamado de baseado em identidade.

- Camada 7: também chamada de *layer 7* no modelo OSI, esta é a camada de aplicação. Corresponde às aplicações (programas) na parte mais elevada da camada OSI, onde e feita a interação entre o computador e o usuário da aplicação. Esta camada também especifica qual protocolo a aplicação utiliza para que aconteça a comunicação. Sete são as do modelo OSI, sendo elas: física, enlace, rede, transporte, sessão, apresentação e aplicação. O conceito da sétima camada de rede é a ferramenta ter capacidade de bloquear uma aplicação específica sem interferir nas demais. Exemplo: conseguir bloquear somente o bate papo de

uma rede social como o *Facebook*, ou bloquear somente a transferência de conteúdo multimídia em uma aplicação como o *WhatsApp*. Isto proporciona proteção avançada e com controle por aplicação.

- Relatórios: que gerasse relatórios detalhados de acesso, consumo de banda de forma individual e geral. Esses relatórios detalhados baseados em identidade é uma forma de inteligência embarcada que nos ajudam na tomada de decisão, de qual conteúdo bloquear ou liberar, quais os riscos oferecidos pelos acessos, quais os países em que foram realizadas mais buscas.

- Tráfego: que a ferramenta suportasse o tráfego de toda rede e filtro de conteúdo passando por ela e que estivesses preparada para futuras ampliações sem precisar de alterações ou redimensionamentos.

- Suporte: além de todos os requisitos citados anteriormente um ponto decisivo para a escolha da ferramenta foi o suporte próximo e disponível pelo menos oito horas por dia e cinco dias por semana. Este, foi fundamental no momento de decidir a escolha da ferramenta.

### 3.2. O UTM escolhido

A ferramenta escolhida na pesquisa: na ferramenta Google *Trends* que gera gráficos com as pesquisas mais realizadas por termo. Para fins de pesquisa, foram escolhidos três dos UTM Firewalls mais pesquisados na atualidade e podemos perceber um sensível aumento na busca pela ferramenta da marca Cyberoam, conforme demonstra o gráfico abaixo:

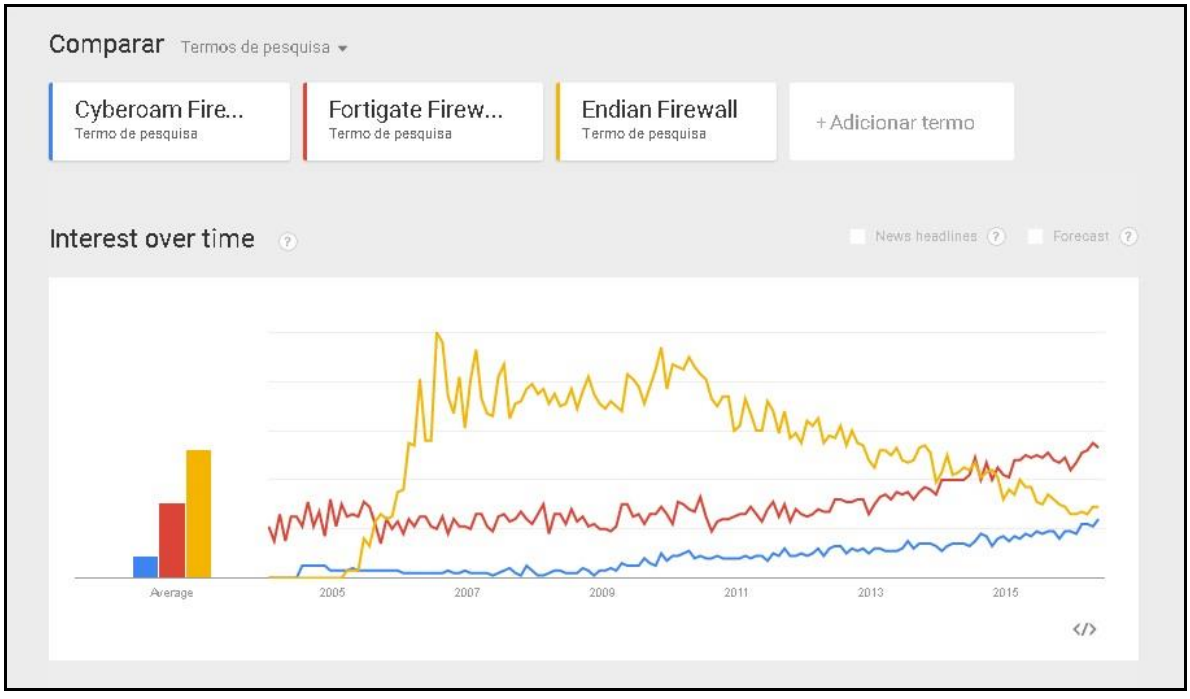



Figura 5 - Gráfico dos UTM mais pesquisados
Fonte: http://www.google.com.br/trends

Sendo assim, o presente estudo de caso foi baseado na implementação da ferramenta específica UTM Cyberoam em uma infraestrutura de Tecnologia da Informação (TI) da prefeitura municipal do município de Faxinal do Soturno utilizando o UTM da marca Cyberoam, com o objetivo de implantar uma infraestrutura de segurança.

A ferramenta Cyberoam é um *firewall* de software e hardware, ou seja, além de ter o ter seu sistema desenvolvido pelo fabricante, ainda conta com o hardware embarcado. Dessa forma, com o equipamento desenvolvido para esse fim em específico, ele foi testado, preparado para trabalhar com grande número de dados (tráfego intenso) e desta forma, está menos sujeito a falhas tanto físicas quanto de software.

Devido ao número de usuários da rede de computadores não ser muito elevado foi escolhida a ferramenta Cyberoam modelo CR25iNG que possui quatro interfaces de rede gerenciáveis que atendem às exigências de recursos. Assim, caso seja feita alguma expansão no número de computadores conectados na rede, não será necessário *upgrade* da ferramenta. Os modelos vão desde os mais básicos para pequenos escritórios ou empresas até os mais robustos, capazes de trabalhar com recurso de alta disponibilidade (mais de um ao mesmo tempo), estes podem atender até a infraestrutura de bancos monetários.

## 4. Implantação do UTM na Infraestrutura de Segurança

O primeiro passo antes da implementação foi definir o escopo do projeto, onde faz-se necessário um desenho esquemático das localidades a serem interligadas, de modo que todo gerenciamento fique unificado em um só ambiente. O desenho pode ser visto na figura 6 a seguir:

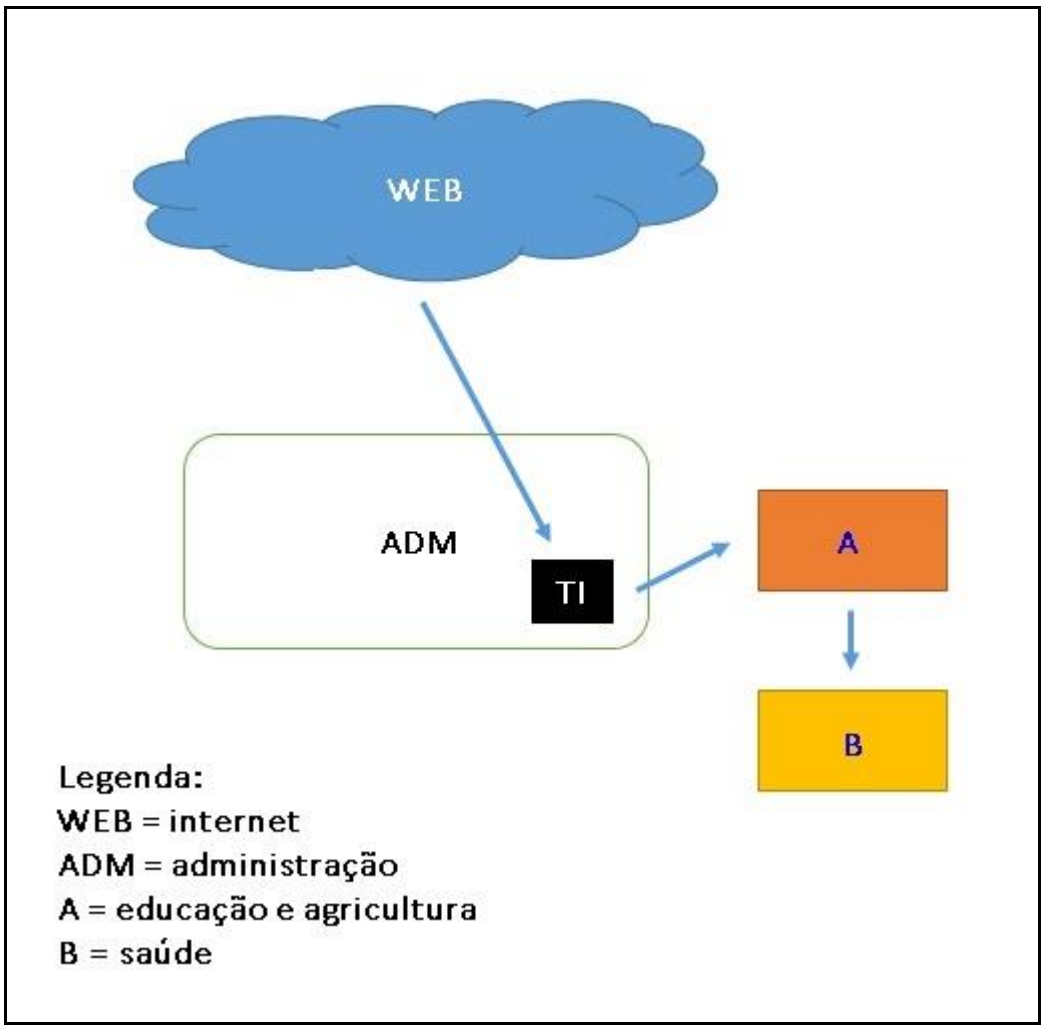



Figura 6 – Esquema do ambiente

A segunda ação tomada durante a implantação da ferramenta no ambiente é dividir a rede, sempre observando o escopo do projeto e respeitando a disponibilidade do ambiente de trabalho, para que a migração de ferramenta gere o menor impacto possível

Dividir uma rede significa separá-la por partes, de acordo com a necessidade de desempenho, nível de acesso ou segurança em padrões pré-estabelecidos. Nesse ambiente, a rede de computadores estava dividida em WAN, DMZ e LAN.

Na figura 7 podemos ver a divisão da rede desta infraestrutura em DMZ, WAN e LAN:

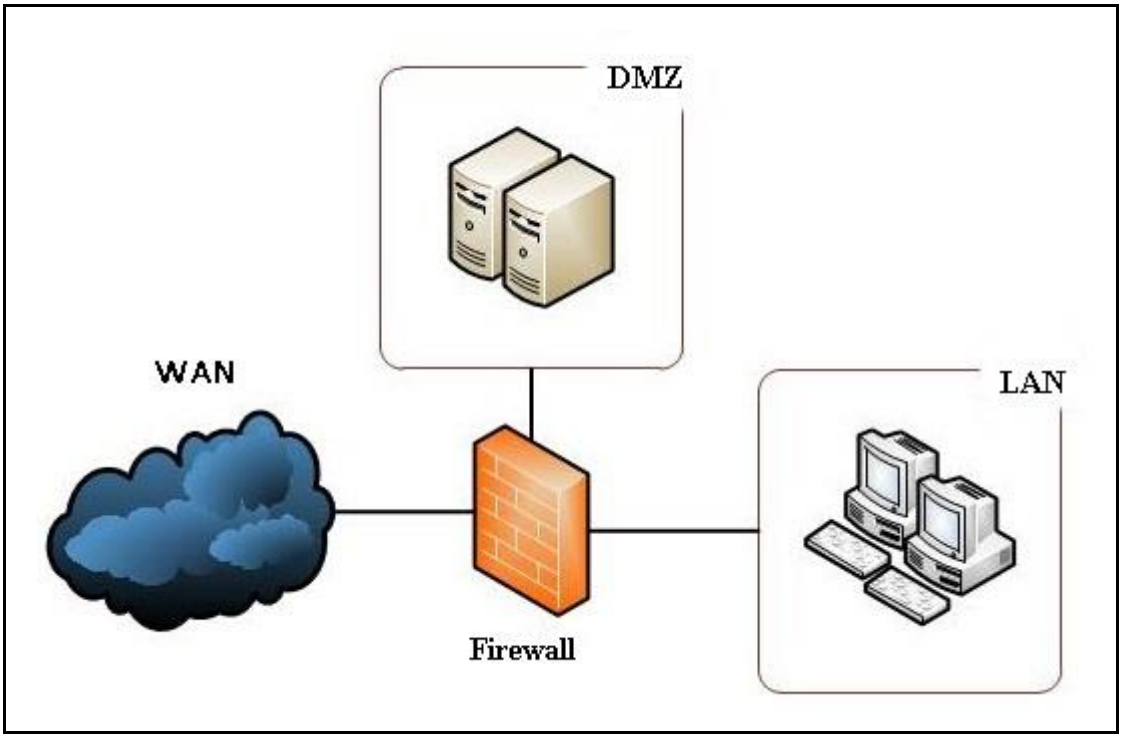



Figura 7 – Modelo padrão de divisão de uma rede

Então, foram configuradas as interfaces de rede, duas interfaces foram destinadas para WAN, pois por questões de disponibilidade o ambiente recebe internet de dois provedores distintos. A seguir, uma interface foi destinada para a LAN e a outra para a DMZ que é onde ficam os servidores. Podemos ver maiores detalhes sobre as interfaces na figura 8:

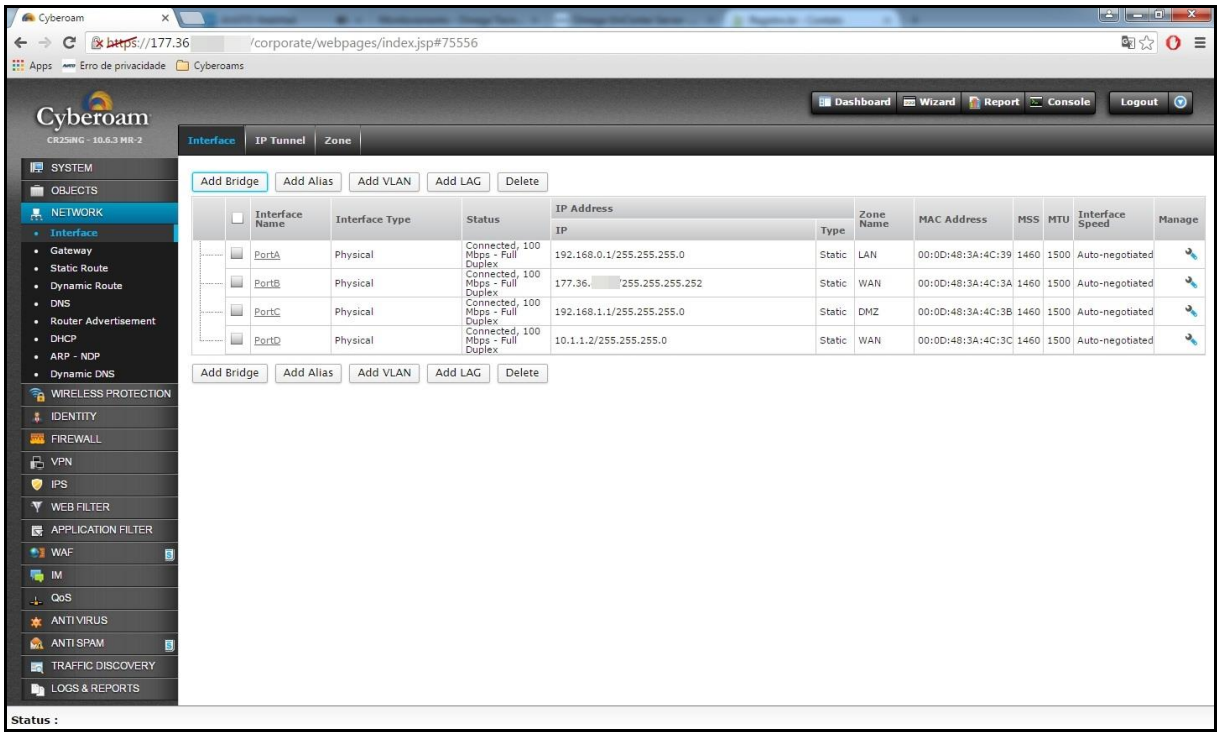



Figura 8 – Configuração das interfaces de rede

Após essa etapa de configuração da ferramenta foram iniciados os trabalhos no ambiente com a lista de usuários previamente cadastrados (*login* e senha), porém não foi feito nenhum bloqueio de conteúdo. Passada uma semana foi feita a verificação dos conteúdos acessados, quais eram mais arriscados e quais páginas eram mais visitadas durante o expediente, bem como o consumo de dados internet utilizado por cada usuário e consumo o total de dados.

Implementando a lista de usuários (controle baseado em identidade) por padrão os usuários foram criados com “nome.sobrenome” com suas devidas senhas individuais. O objetivo de criar usuários é gerenciar o que cada um deles pode acessar de conteúdo web, aplicações web, velocidade de tráfego que cada um terá, geração de relatórios de acesso, consumo e páginas mais visitadas. Esses dados ficam registrados por seis meses no disco do equipamento.

A partir dessas informações pôde ser feito o filtro de conteúdo e avaliação do risco oferecido por algumas das páginas acessadas, de forma individual (baseada em identidade), conforme podemos observar figura 9:

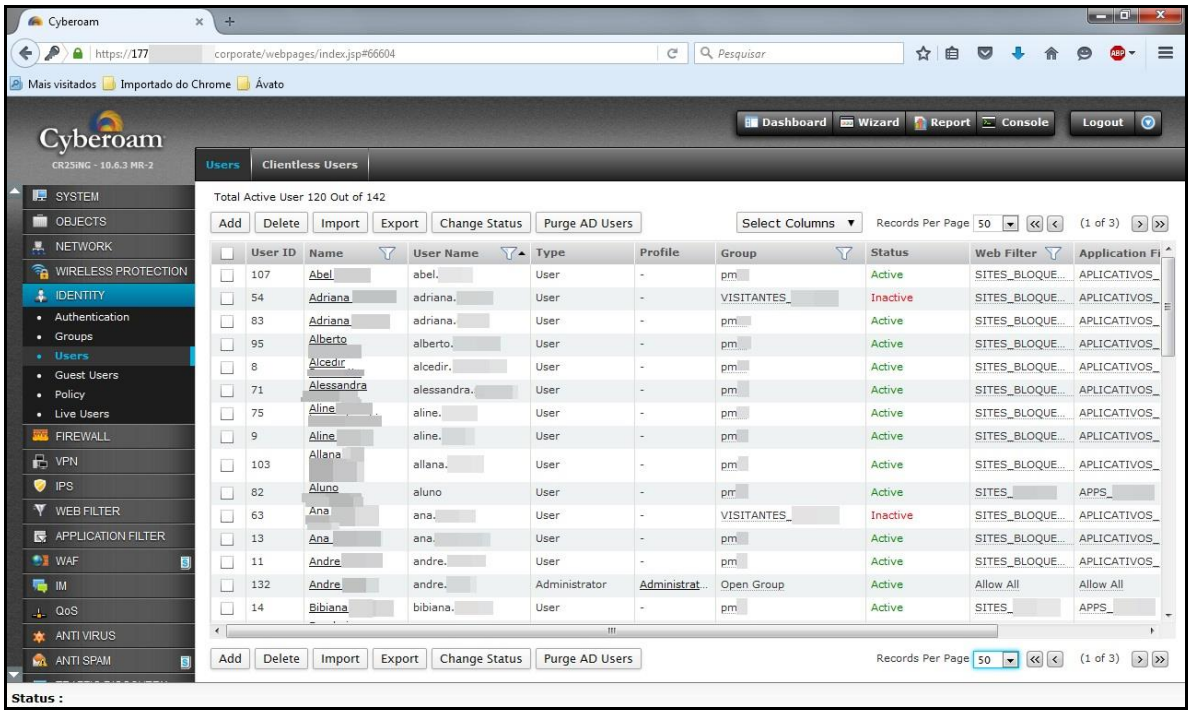



Figura 9 – Painel onde são criados os usuários

Ao clicar em cima do nome de qualquer usuário, vemos a seguinte tela onde definimos regras para eles, estas regras podem ser aplicadas por grupo ou de forma individual. Nesta tela pode ser estipulado um horário de acesso, acessos simultâneos e também é cadastrado um e-mail e senha.

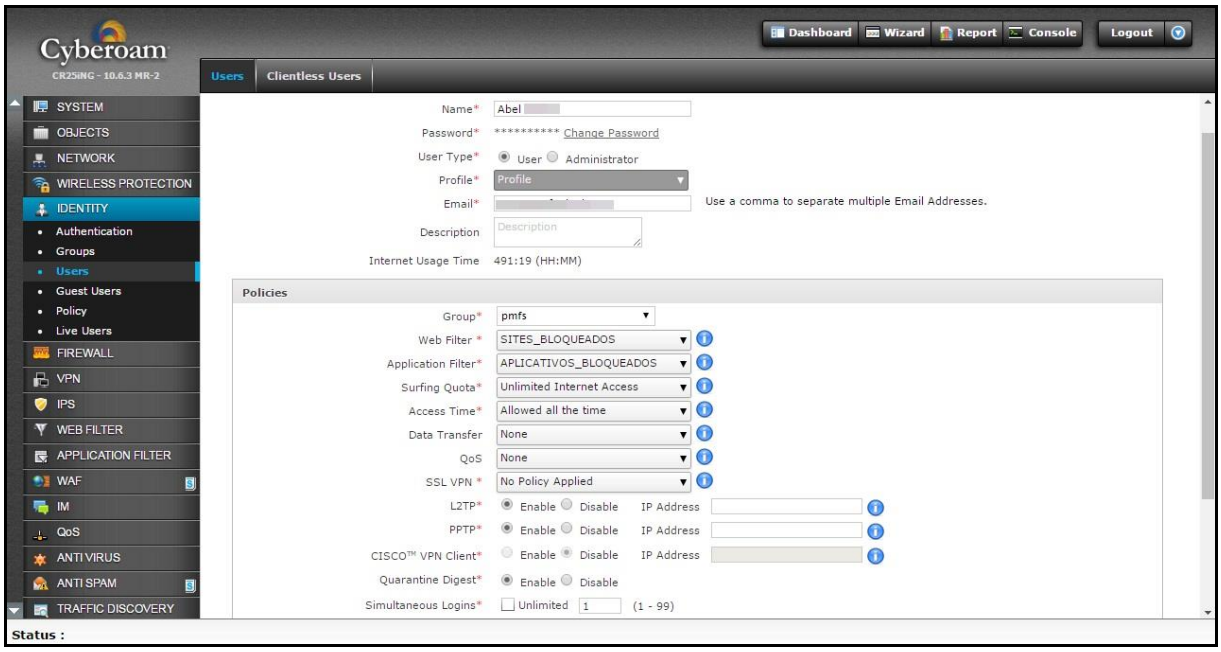



Figura 10 - Regras aplicadas ao usuário ou grupo

A figura 11 representa o painel principal da interface web da ferramenta, onde podem ser visualizados os detalhes sobre consumo de recursos (processador e memória), bem como status dos links de internet e detalhes sobre o equipamento.

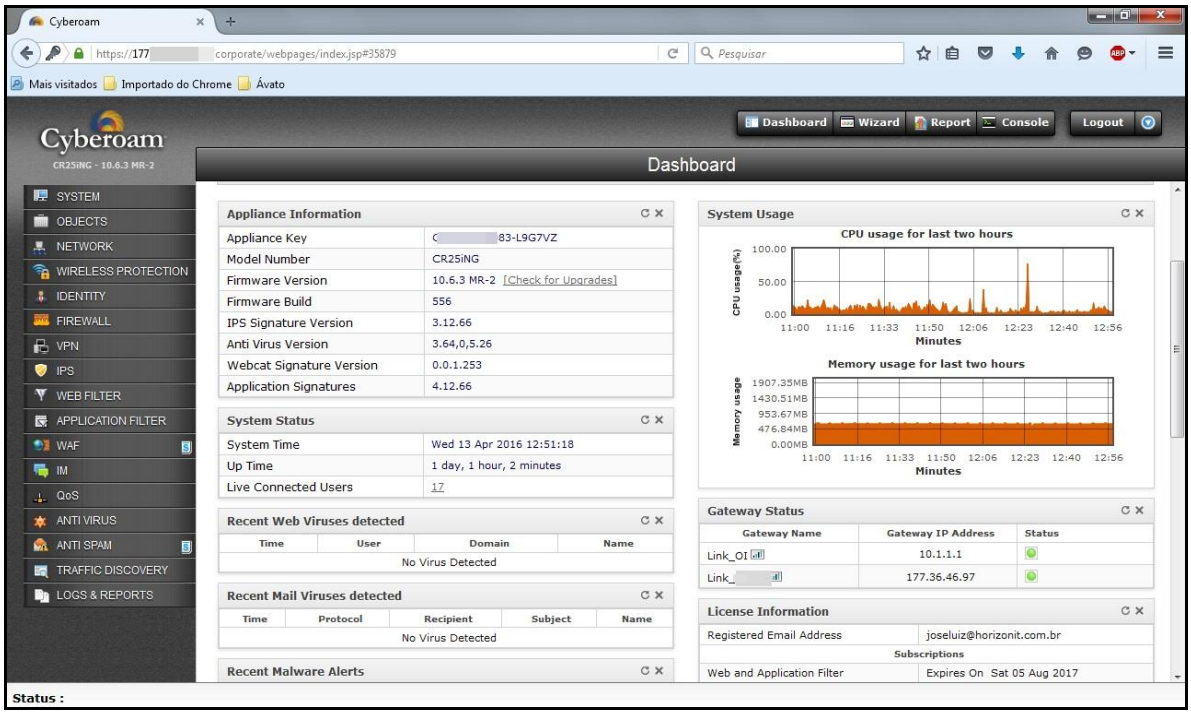



Figura 11 – Painel principal do UTM *Firewall*

## 4.1. Filtro Web

No filtro Web, também conhecido como *Proxy* pode ser permitido ou negado acesso aos sites acessados na internet. Resumidamente, é aqui que inicia a segurança do ambiente, pois pode ser bloqueado qualquer tipo de conteúdo web que possa ser prejudicial ao ambiente.

No filtro de páginas Web tem-se categorias, estas categorias são oriundas de uma lista de classificação presentes na própria ferramenta, onde são periodicamente atualizadas de forma automática. Exemplo: entretenimento, comércio, redes sociais, conteúdo adulto. As categorias padrão não podem ser alteradas, apenas removidas ou adicionadas às políticas de acesso. Já, caso seja necessário, podem ser criadas categorias com a preferência ou necessidade do gestor do ambiente, com ação de bloquear ou permitir. As categorias podem ser vistas na figura 12:

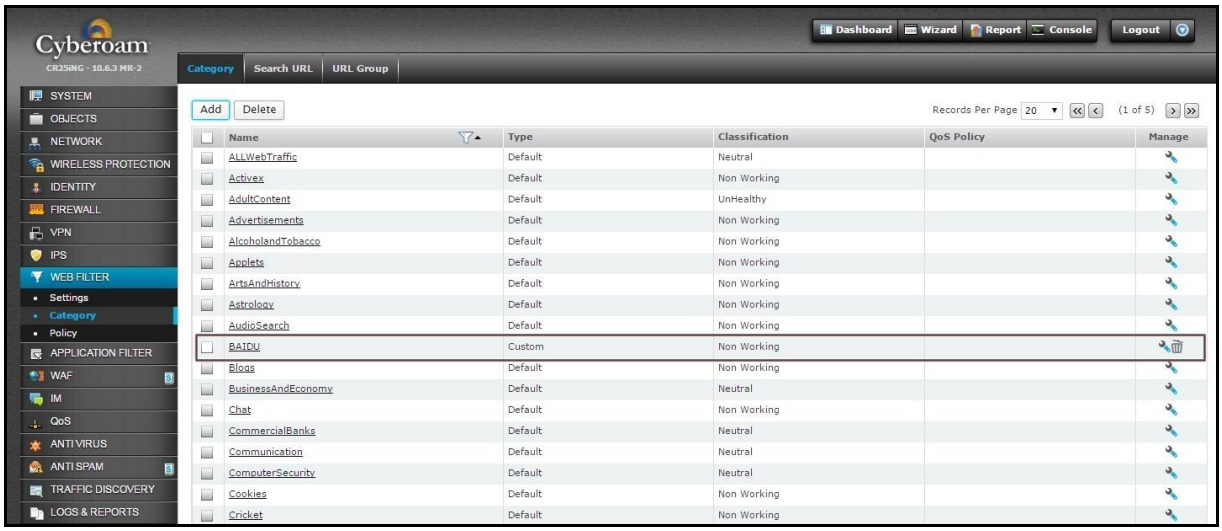



Figura 12 – Categoria customizada

Estas categorias web são gerenciáveis, é possível criar categorias específicas com o endereço dos sites desejados, o sistema faz isso através de endereços de domínio ou palavras-chave, conforme ilustradas na seguinte tela:

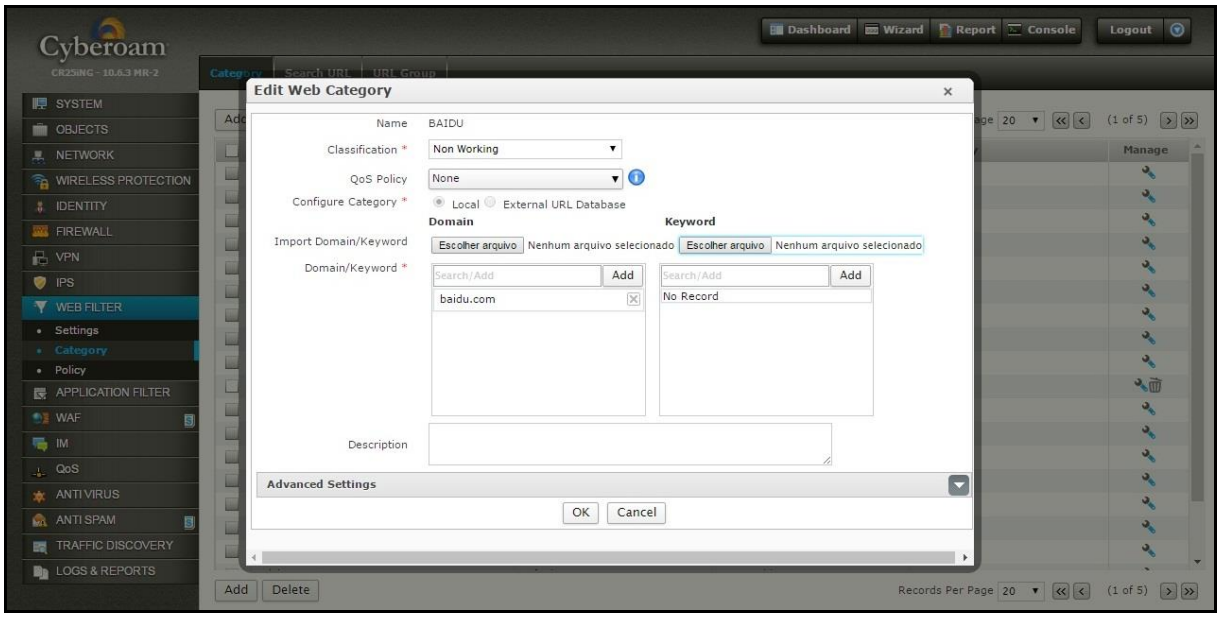



Figura 13 - Criando uma categoria customizada

Com os usuários criados e as categorias definidas a configuração parte para as políticas do filtro web. Aqui as políticas são criadas com as suas devidas categorias vistas anteriormente, ou seja, dentro de cada política existem categorias de páginas Web podendo ser padrão ou customizadas. Podemos ver as políticas de com suas categorias na figura 14:

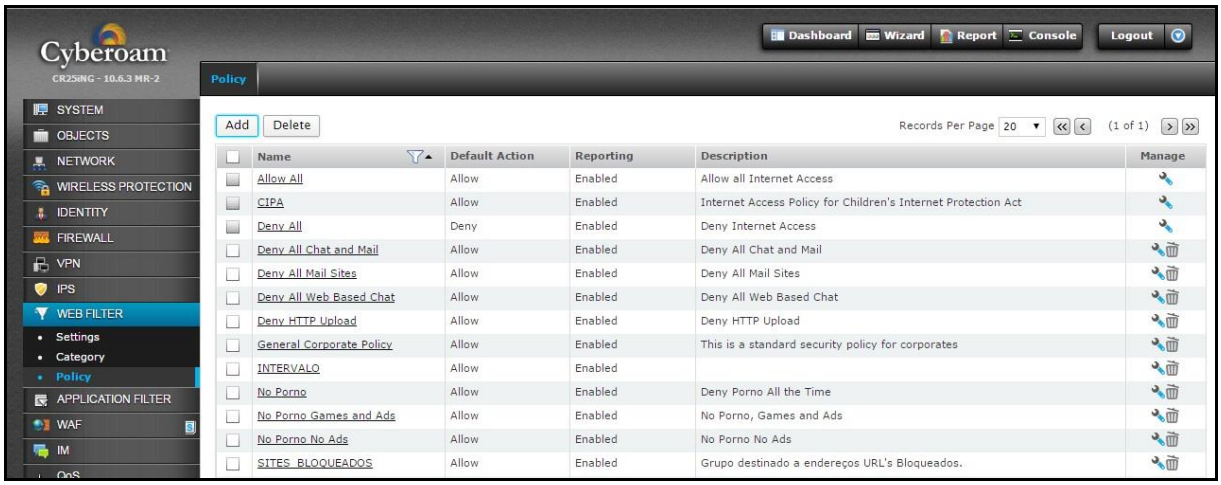



Figura 14 - Políticas de acesso Web

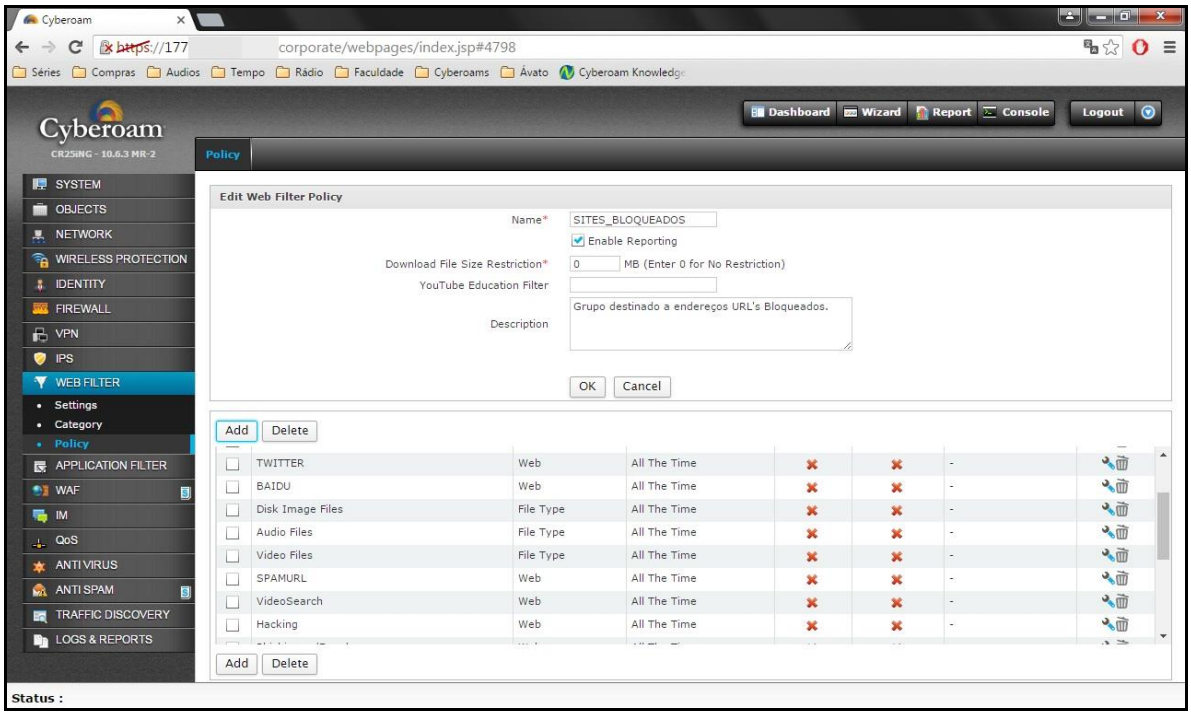



Figura 15 - Categorias vistas dentro da política de bloqueio

## 4.2. Filtro de Aplicação

Fazer o bom uso da Web é essencial no cumprimento das tarefas diárias, porém é necessário ter uma ferramenta específica para este fim. Além do filtro Web o UTM ainda conta com o recurso de filtro de aplicações, este filtro atua monitorando diretamente o que passa pela camada de aplicação também conhecido como *layer* 7, onde podem ser escolhidas quais aplicações serão permitidas ou bloqueadas.

Vários protocolos operam nessa camada, cada um é responsável por um tipo de serviço, esta é a camada que “conversa” com os programas do computador ou dispositivo que faz uso da rede e é nela que pode ser bloqueada apenas uma aplicação específica (TORRES GABRIEL, 2013). Por exemplo: bloquear somente a chamada de voz do *whatsapp* ou sua transferência de imagens e vídeos de forma específica.

Podemos visualizar a lista de aplicações na figura 16:

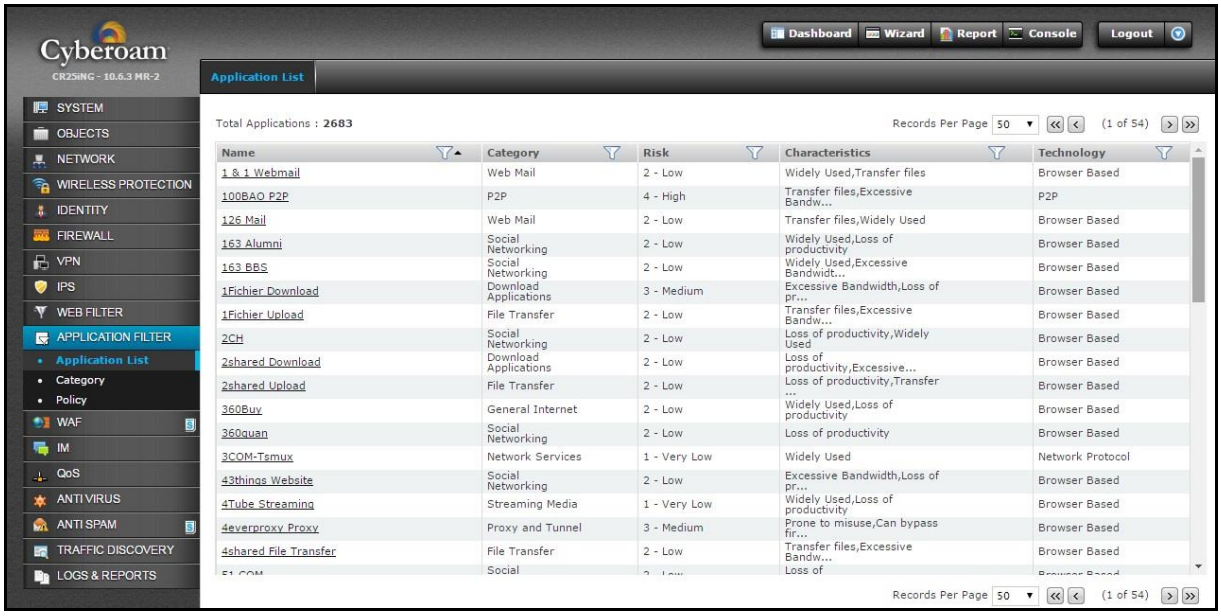



Figura 16 - Lista de aplicações contidas no sistema

Assim como no filtro web, as categorias de aplicação são divididas por categorias e também são atualizadas automaticamente. Representamos as categorias de aplicação na figura 17:

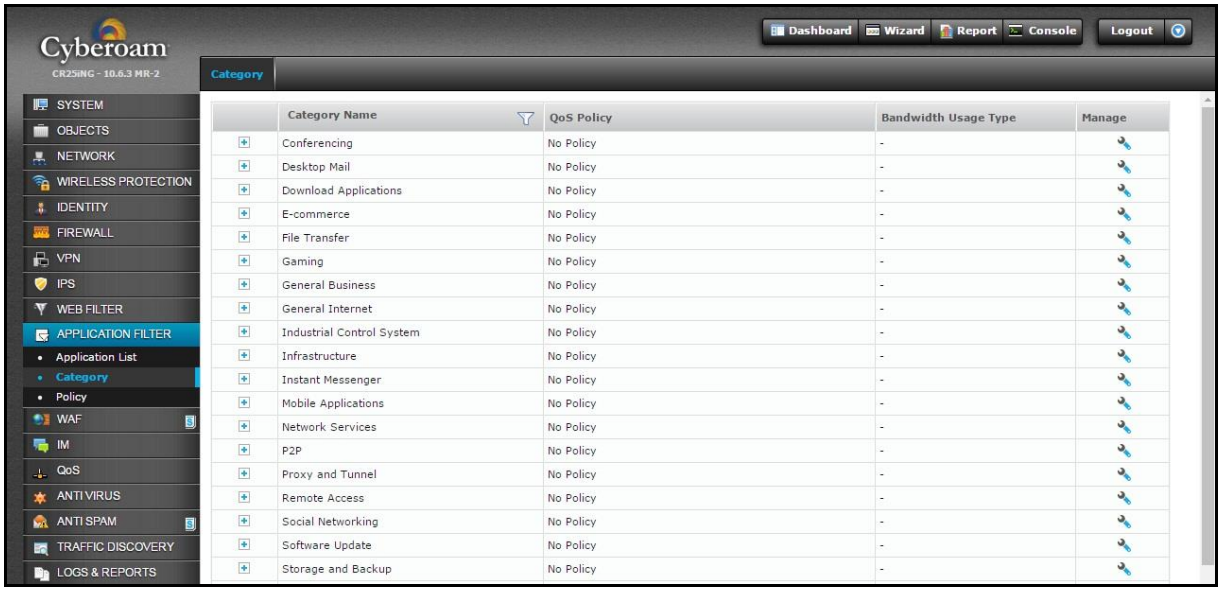



Figura 17 - Categorias de aplicação

É importante destacar que as políticas de aplicação com suas devidas categorias podem ser customizadas, porém as categorias de aplicação não podem. Na figura 18 representamos as políticas de aplicação, que foram criadas.

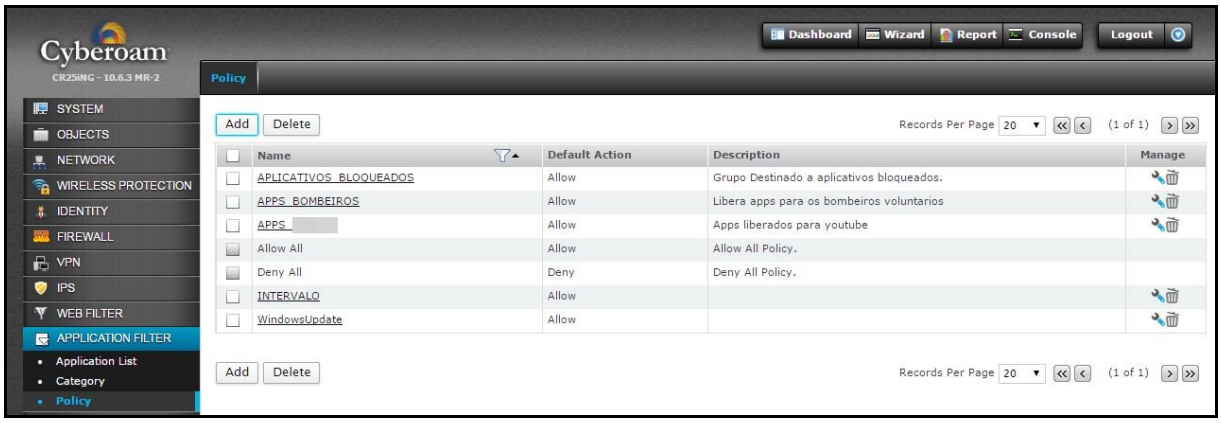



Figura 18 – Políticas de aplicação

Na figura 19 pode ser visualizado o que foi adicionado dentro da política de acesso à aplicação "APLICATIVOS_BLOQUEADOS". Conforme podemos observar na imagem abaixo, foram bloqueadas algumas categorias referente a redes sociais e também tráfego de áudio .MP3.

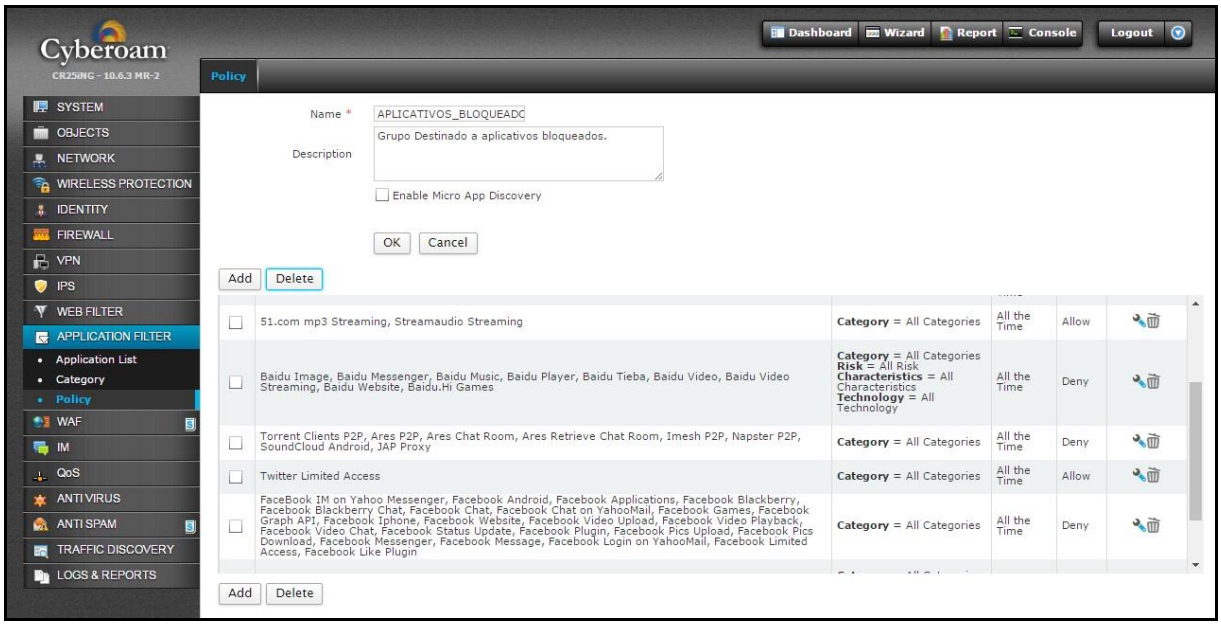



Figura 19 - Interior das políticas de aplicação

## 4.3. Aplicando os Filtros

Até agora foi visto como funcionam as os filtros web e de aplicação. Mas onde isso é colocado em prática para finalmente efetivar os bloqueios?

No *firewall*. Quem irá permitir ou negar todas as regras previamente configuradas é o *firewall* da ferramenta UTM. Dentro dele existem regras que podem ser parametrizadas para cada zona da rede (LAN, DMZ, WAN). Os bloqueios de acesso para a maioria dos casos são realizados no tráfego da zona LAN para a WAN. A figura 20 representa isso:

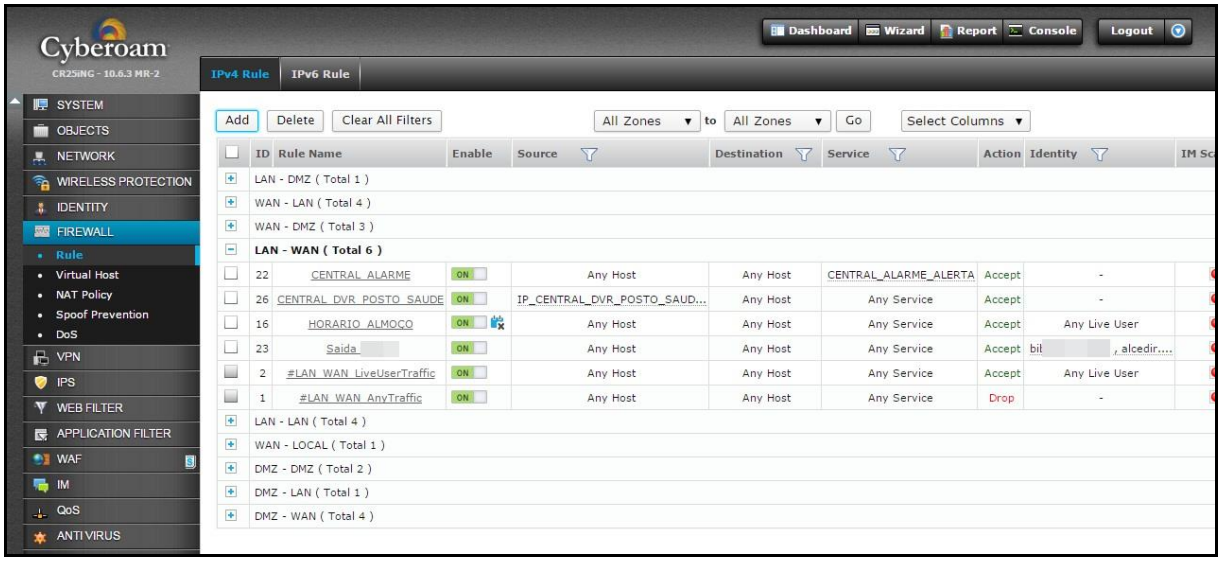



Figura 20 - Regras de *firewall* de LAN para WAN

A seguir é demonstrado o que é definido dentro da principal categoria, que representa o tráfego real da rede, e representada pelo nome *"#LAN_WAN_LiveUserTraffic*":

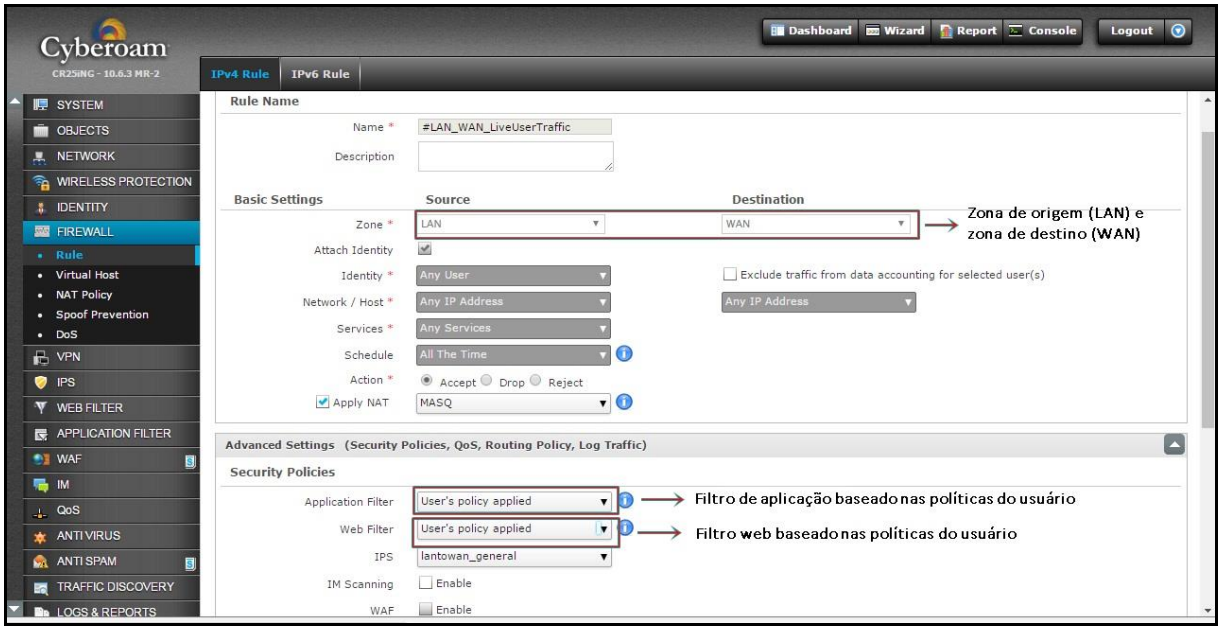



Figura 21 - Interior de uma regra de *firewall*

### 4.4. Redirecionamentos

Como a necessidade de acesso externo através dos serviços de área de trabalho remota do Windows, foram criados os redirecionamentos. Um redirecionamento funciona da seguinte forma: ao informar o endereço IP da rede WAN e sua devida porta no assistente de conexão de área de trabalho remota, ele irá fazer uma busca na rede a procura da porta especificada liberada para acesso, então ele passa para a interna que por sua vez possui um IP interno (da rede LAN).

Todo esse processo tem que passar pelo *firewall* da zona WAN para LAN. A figura 22 ajuda a entender melhor o processo de redirecionamento:

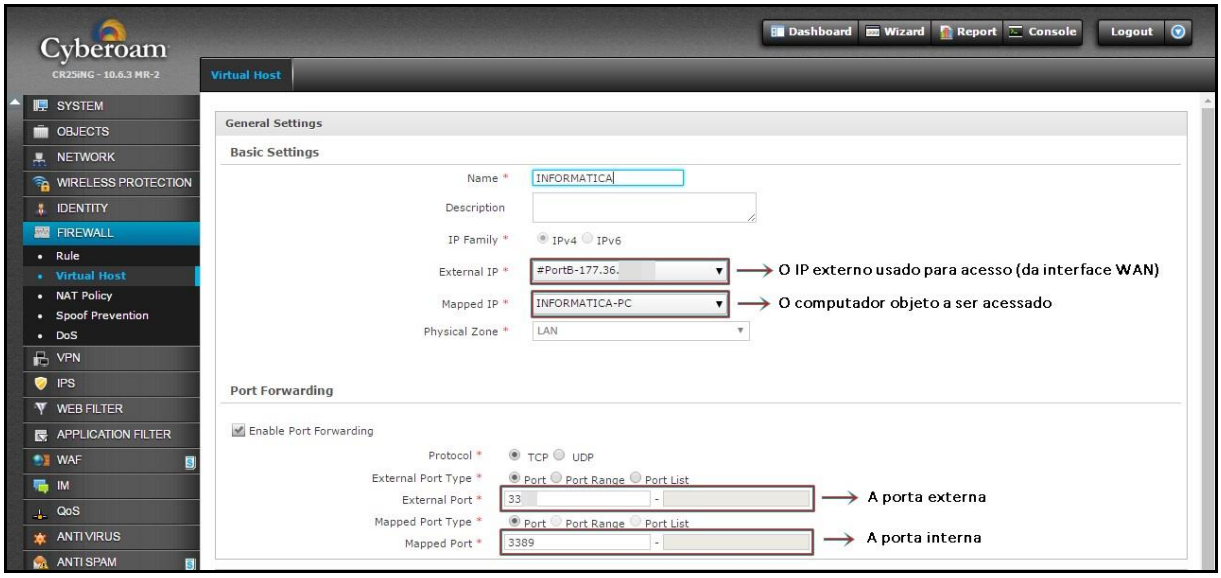



Figura 22 - Redirecionamento de portas

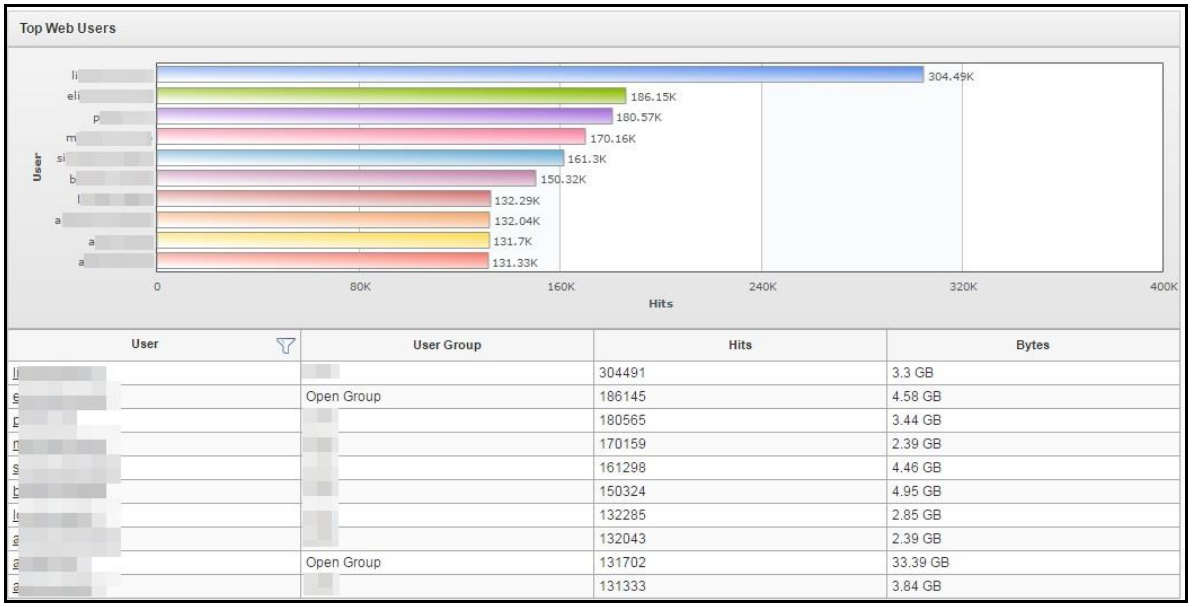
## 5. Resultados Obtidos

Foi constatada uma considerável queda tráfego internet que antes era desperdiçado com o acesso a aplicações e páginas não produtivas tais como: vídeos, jogos on-line, músicas e rádios. Além da diminuição do tráfego internet obtido através dos filtros web e de aplicação, o UTM ainda contribui para monitoramento em tempo real da quantidade de usuários autenticados, horário, tentativas de ataque externa, vírus na rede e transferência de download/upload. Além do mais, podem ser feitos bloqueios por endereço físico (MAC), criar rede virtual privada (VPN) bem como redirecionamento de portas para acesso remoto externo aos servidores.

Abaixo foram obtidos os seguintes gráficos pelo I-View que é a ferramenta de relatório utilizada por esse fabricante no período de 04-04-2016 até 08-06-2016:

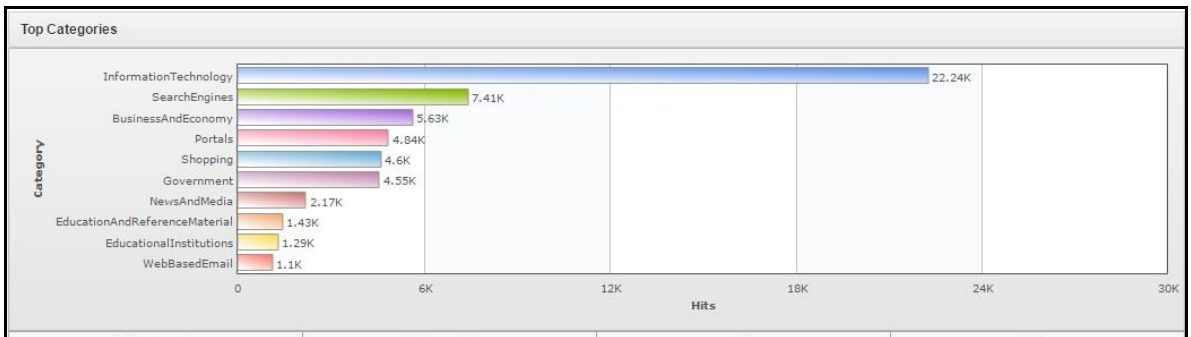
- Usuários que mais consumiram banda;
- Categorias de Web Sites mais acessadas;
- Aplicações mais bloqueadas;

- Países em que as pesquisas foram mais destinadas.



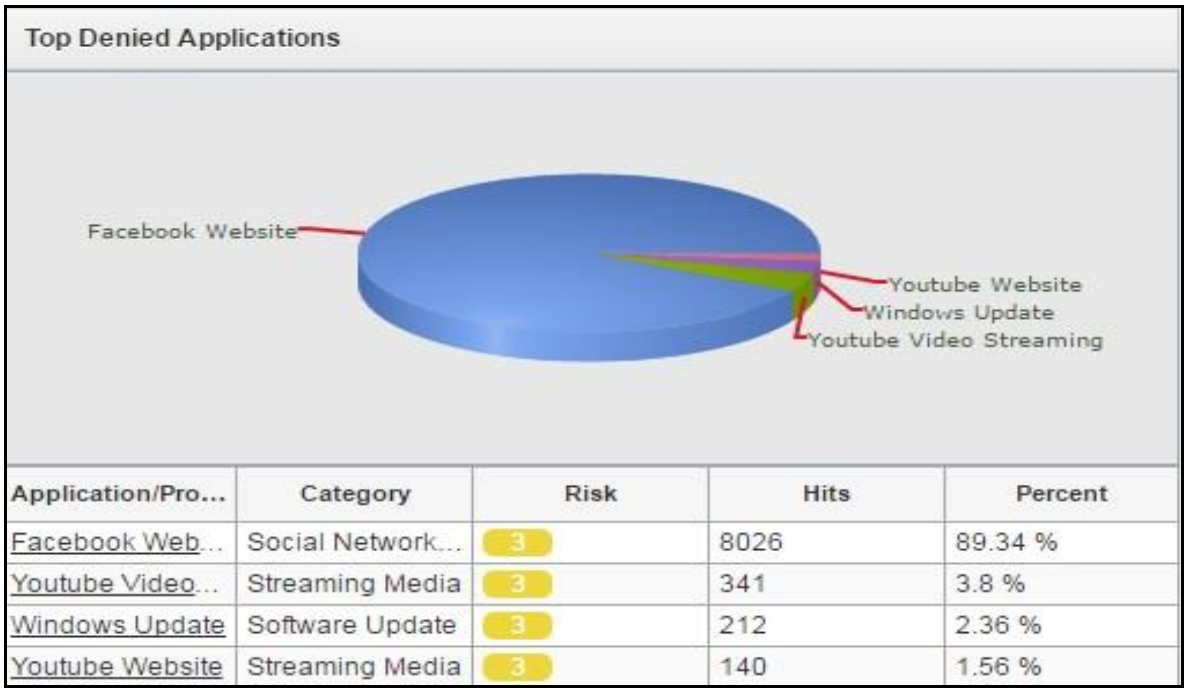

| User | User Group | Hits | Bytes |
|---|---|---|---|
| [redacted] | [redacted] | 304491 | 3.3 GB |
| [redacted] | Open Group | 186145 | 4.58 GB |
| [redacted] | [redacted] | 180565 | 3.44 GB |
| [redacted] | [redacted] | 170159 | 2.39 GB |
| [redacted] | [redacted] | 161298 | 4.46 GB |
| [redacted] | [redacted] | 150324 | 4.95 GB |
| [redacted] | [redacted] | 132285 | 2.85 GB |
| [redacted] | [redacted] | 132043 | 2.39 GB |
| [redacted] | Open Group | 131702 | 33.39 GB |
| [redacted] | [redacted] | 131333 | 3.84 GB |

Figura 23 – Usuários que mais consumiram banda



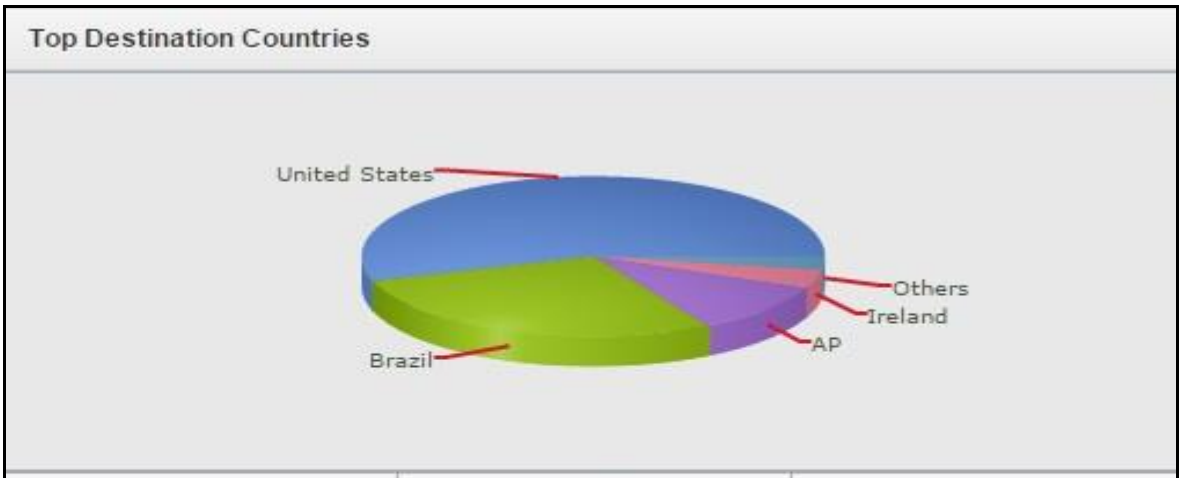

| Category | Category Type | Hits | Bytes |
|---|---|---|---|
| InformationTechnology | Neutral | 22241 | 1.57 GB |
| SearchEngines | Neutral | 7409 | 252.39 MB |
| BusinessAndEconomy | Neutral | 5631 | 123.32 MB |
| Portals | Non Working | 4843 | 105.53 MB |
| Shopping | Non Working | 4602 | 71.8 MB |
| Government | Neutral | 4545 | 152.73 MB |
| NewsAndMedia | Neutral | 2173 | 23.65 MB |
| EducationAndReferenceMaterial | Neutral | 1433 | 76.55 MB |
| EducationalInstitutions | Neutral | 1285 | 94.07 MB |
| WebBasedEmail | Non Working | 1096 | 48.31 MB |

Figura 24 – Categorias da Web mais acessadas




| Application/Pro... | Category | Risk | Hits | Percent |
|---|---|---|---|---|
| Facebook Web... | Social Network... | 3 | 8026 | 89.34 % |
| Youtube Video... | Streaming Media | 3 | 341 | 3.8 % |
| Windows Update | Software Update | 3 | 212 | 2.36 % |
| Youtube Website | Streaming Media | 3 | 140 | 1.56 % |

Figura 25 – Aplicações com maior número de bloqueios.




| Country | Bytes | Percent |
|---|---|---|
| United States | 4.72 GB | 54.82 % |
| Brazil | 2.46 GB | 28.57 % |
| AP | 905.96 MB | 10.27 % |
| Ireland | 326.46 MB | 3.7 % |
| Others | 233.84 MB | 2.65 % |

View All

Figura 26 – Países que tiveram as pesquisas mais destinadas.

A figura 27 é um gráfico representando queda de tráfego (imagem obtida através do monitoramento do provedor de acesso Ávato).

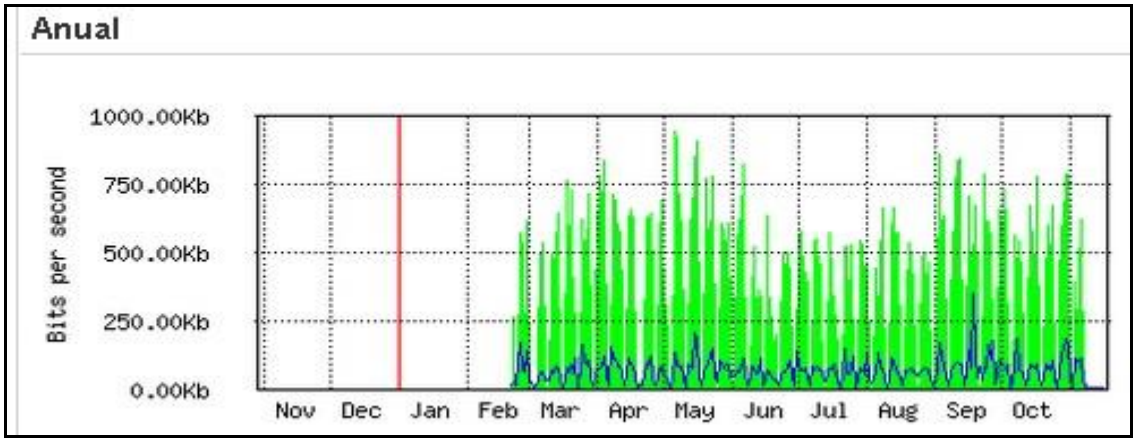



Figura 27 – Queda de tráfego

A figura 28 representa a ferramenta UTM Firewall da marca Cyberoam modelo CR25iNG *(appliance)* que foi implantada na infraestrutura de segurança que é objeto dessa pesquisa acadêmica.


Figura 28 – CR25iNG *(appliance)*
Fonte: https://www.cyberoam.com/images/CR25iNGAppliance.png

Ainda, para acrescentar um pouco mais à essa pesquisa, foi coleto o depoimento de alguns servidores públicos de diferentes setores, estes depoimentos foram obtidos através dos formulários do Google, onde o link de pesquisa foi disponibilizado para os colaboradores por e-mail com a seguinte pergunta:

**Qual a sua percepção do ambiente de trabalho após a implantação das políticas de acesso (bloqueios)? Responda em um breve parágrafo.**

“Ótimo, pois assim a internet será usada realmente só para o trabalho, não excedendo a banda com conteúdo indevido, consumindo recursos com Facebook e downloads de conteúdo não relativo ao trabalho durante o expediente.”

“Acredito que o saldo seja positivo. Obviamente, para quem sabe usar de maneira saudável, não seria necessário esse tipo de restrição. Entretanto, como há muita gente que não sabe utilizar de maneira coerente as liberdades que são dadas, vejo que estas políticas servem como uma "tranquilidade" no ambiente de trabalho.”

“Vejo que segurança em todos os aspectos da nossa vida é importante. No que diz respeito às informações dentro das organizações este tema toma uma relevância maior. Diria imprescindível para a organização. Tornam o trabalho mais sério, buscam maior compromisso e comprometimento dos colaboradores, tempo melhor aproveitado.”

## 6. Considerações Finais

Com esse trabalho de pesquisa podemos considerar que um UTM Firewall possivelmente é uma das melhores soluções presentes no mercado para gerenciar ambientes corporativos.

Utilizando UTM vemos como fica mais fácil para um gestor e TI, criar e gerenciar políticas de acesso, redirecionamentos, consultar relatórios de consumo, páginas mais acessadas além de evitar que pessoas não autorizadas usem a conexão do ambiente para aceso à internet.

Também podemos perceber que houve uma considerável queda tráfego internet que antes era desperdiçado com o acesso a aplicações e páginas não produtivas tais como: vídeos, jogos on-line, músicas e rádios.

# Referências

**Appliance (MORIMOTO E. CARLOS, 2005)**
Disponível em: http://www.hardware.com.br/termos/appliance
Acessado em 20-01-2016.

**Cyberoam - Comprehensive Security from Layer 2 to Layer 8**
Disponível em: http://www.cyberoam.com/networksecurity.html
Acessado em 12-11-2014.

**Fortinet - Soluções e Segurança UTM**
Disponível em: http://www.penso.com.br/solucoespenso/fortinet-seguranca-utm/
Acessado em 10-11-2014.

LIMA, Gustavo. **Vocês já ouviram falar no Web Application Firewall (WAF)**?
Disponível em: http://blog.corujadeti.com.br/voces-ja-ouviram-falar-no-web-application-firewall-waf/
Acessado em 30/10/2014.

**Livro Redes de Computadores (TORRES GABRIEL, 2013)**

**MICROSOFT. O que é um firewall?**
Disponível em: http://windows.microsoft.com/pt-br/windows/what-is-firewall#1TC=windows-7
Acessado em 10/11/2014.

O que é Firewall? **(Infowester)**
Disponível em: http://www.infowester.com/firewall.php
Acessado em: 02-06-2016

**PortNetwork - Segurança da Informação**
Disponível em: http://www.portnetwork.com.br/Cyberoam.html
Acessado em 10-11-2014.

**SonicWall**
Disponível em: http://www.sonicwall.com/br/pt/products/Network-Security.html
Acessado em 12-11-2014.

**UTM e Firewall de nova geração: conheça as diferenças**
Disponível em: http://www.bspi.pt/notiacutecias/utm-e-firewall-de-nova-gerao-conhea-as-diferenas
Acessado em 10-11-2014.