JORNAL DE ENGENHARIA, TECNOLOGIA E MEIO AMBIENTE
Nº 2. Vol. 1 2017/1

CONTROLE DE BANDA DE INTERNET POR GRUPOS DO ACTIVE DIRECTORY

Rodrigo de Sousa Ribeiro[1]; Diovani dos Santos Milhorim.[2]; Eduardo Fernandes Saad[3]

[1,2,3] Faculdade de Talentos Humanos, Uberaba (MG), Brasil

rodrigorsr993@gmail.com, diovani.milhorim@facthus.edu.br, eduardo.saad@facthus.edu.br.

RESUMO: O consumo de banda indevido dentro de uma empresa é um grande problema hoje, pois uma rede sem controle pode causar lentidão e dificultar o trabalho. O objetivo do presente artigo é mostrar uma maneira de controlar a banda e o acesso à internet utilizando ferramentas que são comuns dentro das empresas nos dias de hoje como o *Active Directory* (sistema de gerenciamento de usuários e computadores) e o *proxy Squid* (sistema de gerenciamento de acesso à internet e redes externas). Para realização do projeto foram utilizadas máquinas virtuais através do software *Vmware Workstation*, com os sistemas operacionais Ubuntu Server 14.04, Windows Server 2008 R2 e Windows 7. Foram configurados os serviços Squid, BIND (serviços de resolução de nomes), DHCP *Server* (serviço de endereço de redes dinâmico), *Active Directory* através de protocolos LDAP com a integração do Squid e o *Active Directory*. O controle de banda foi obtido com o uso do recuso *Delay Pools* do próprio squid. O projeto mostrou-se promissor pelo fato de outras ferramentas de controle de banda não terem possibilidades de controle por usuário.

PALAVRAS CHAVE: AD, controle de banda, Squid.

INTERNET BANDWIDTH CONTROL BY GROUPS OF ACTIVE DIRECTORY

ABSTRACT: Consumption of improper bandwidth within a company is a major problem today, because an uncontrolled network may cause slowness and hinder the work. The objective of this article is to show a way to control the internet bandwidth and access using tools that are common within companies today such as the AD and Squid. To do so, virtual machines through the Vmware Workstation software were used, In these machines, an Ubuntu Server 14.04, Windows Server 2008 R2 and a Windows 7 were installed. Squid, Bind, Dhcp Server, Active Directory services were configured through LDAP protocols with the integration of Squid and Active Directory, obtaining the bandwidth control with the Delay Pools. The project proved to be very promising because other bandwidth control tools have no possibility of user control.

KEY WORDS: AD, Squid, Internet bandwidth.

INTRODUÇÃO

A ideia da internet surgiu na década de 1960, ainda chamada ARPANET em 1967 quando se interligou quatro nós de redes. Em 1972 parte do grupo que criou a ARPANET colaborou em um projeto chamado Internetting Project para interligar redes distintas. Mas a explosão da internet aconteceu em 1990 com a criação do *World Wide Web* (WWW) que popularizou a internet pelo mundo. (FOROUZAN, MOSHARRAF, 2013). Atualmente, existem mais de 3,2 bilhões de usuários pelo mundo. Estima-se que ainda 4,1 bilhões de pessoas não tenham acesso à internet. (FBNEWSROOM, 2016)

O consumo de banda de internet dentro de um ambiente corporativo é um dos grandes problemas das empresas nos dias de hoje. Qualquer usuário sem noções de ética pode requisitar grandes cargas de dados ou acessar sites indevidos, prejudicando toda a rede com o mau uso de internet comprometendo significativamente os acessos da rede interna.

Uma maneira de resolver este problema é através do controle de banda. Existem algumas ferramentas de controle de banda como o WebHTB, Switchs Gerenciáveis, Roteadores sem fio e o recurso *Delay Pools* do *proxy* Squid. Não obstante, foi escolhido o Squid pela possibilidade de integração com um AD (*Active Directory* – serviço de gerenciamento de usários e computadores). Este artigo tem como objetivo fazer um estudo de caso sobre o controle de banda de internet com monitoramento de banda e de acessos de uma rede interna através de grupos do Active Directory. Acessando a internet através de um *firewall* que trabalha com Squid e que utiliza grupos de trabalho de um Servidor de Active Directory. Controlando a banda e o acesso de cada grupo do AD conforme a necessidade da empresa.

MATERIAIS

Software de virtualização Vmware

A virtualização pode ser definida como a criação de um ambiente virtual que simula um ambiente real, permitindo a utilização de diversos sistemas e aplicativos sem a necessidade de acesso físico à máquina que estão hospedados. (AMARAL, 2009)

A VMware é um software de virtualização bem popular pelo seu uso simples e prático. Existem vários softwares desta empresa, sendo a maioria pago como o VMware Workstation, VMware ESXI para servidores e o VMPlaye, sendo este último de uso gratuito. Para a execução do projeto foi utilizado o VMware Workstation. (VMWARE, 2016)

Embora haja softwares de virtualização como o Hyper-V da Microsoft, Virtual Box e o Citrix, elegeu-se o VMware justamente por sua simplicidade.

AD Active Directory

O Active Directory surgiu com a necessidade de o usuário de ter um único diretório, ou seja, ao invés deste ter uma senha para ler e-mail, acessar o sistema da empresa ou identificar-se em uma rede, com a utilização do AD, o usuário pode acessar todos os recursos disponíveis com apenas uma senha. Podemos definir um diretório como um banco de dados que armazena informações de usuários. (MELO, 2014)

O AD é um serviço da Microsoft que permite criar usuários e pastas com permissões restritas além de permitir um maior controle do usuário através de uma GPO (*Group Policy* – grupo de policiamento).

GPO são regras e bloqueios feitos a usuários do AD que são capazes de mudar configurações, restringir ações entre outras funções. Essas regras podem ser aplicadas para grupos separados ou para todos os usuários. (BRANDÃO, 2016)

Squid

Squid é um software para gerenciamento de acesso à internet ou redes externas que permite também armazenar páginas acessadas anteriormente (*cache*). Squid é um programa robusto, simples e confiável. Ele trabalha com ACLs (*Access Lists* – listas de acessos) e realiza o controle de tráfego de internet bloqueando ou permitindo determinado acesso, além de controle de taxa de transmissão de dados e outras regras que podem ser configuradas dentro do Squid. (MARCELO, 2006)

O Squid é baseado em *Cache Daemon*, e para a realização do presente estudo de caso, foi utilizado à versão 3.3 por se tratar de uma versão mais segura e pela sua disponibilização nos repositórios de instalação padrão do Linux.

Um proxy é um servidor HTTP (*Hyper Text Transfer Protocol*) de filtragem de pacotes que aguarda a requisições de computadores da rede interna, repassa estas requisições para o servidor remoto externo, recebendo uma resposta, enviando-a de volta para a estação cliente. (MARCELO, 2006)

DHCP- *Dynamic Host Configuration Protocol*

DHCP é o protocolo que permite que todos os equipamentos de rede recebam um IP único na rede e outras configurações como o DNS (Endereço do servidor de nomes), *Gateway* (roteador de saída da rede), etc... Através do servidor DHCP, pode-se definir que um determinado endereço MAC (endereço físico de rede do adaptador) sempre receba um determinado endereço lógico IP (*internet protocol*). (MACHADO, SOARES, REY, CERON, JÚNIOR, 2009)

Para realização do projeto foi usado o software dhcp-server disponível no sistema operacional Linux.

LDAP- *Lightweight Directory Access Protocol*

O LDAP é formado por um conjunto de protocolos cliente/servidor, utilizado para acessar um determinado diretório e suas informações, permitindo navegar, ler e consultar seus atributos. Diferente de um banco de dados relacional, qualquer cliente LDAP pode obter dados de um servidor LDAP já que não precisa de nenhuma biblioteca específica para implementar este protocolo. A forma de armazenamento dos dados e o sistema operacional base não fazem parte do protocolo (TRIGO, 2007, p.239).

O protocolo LDAP é utilizado como padrão em serviços de diretórios pela possibilidade de ser utilizado em plataformas diferentes. Com o LDAP conseguimos consultar informações sobre os usuários ou grupos de trabalho que ficam armazenados junto à base de dados do servidor. (SANTOS, 2013)

Com ele, cada grupo é carregado no AD em uma variável disponível no Squid, para que seja possível manipular esse grupo como preferir.

IPTables

O IPTables (*Netfilter*) existe no linux desde o kernel 2.4. IPTables é uma ferramenta nativa do sistema operacional Linux que permite a criação de regras no *firewall* e redirecionamento de requisições de rede (NATs - ver tópico seguinte). Ele funciona baseado em endereço e portas de origem e destino, determinando se o pacote solicitado tem ou não permissão para entrar na rede. (MUNIZ, 2014)

NAT

NAT (*network address translation*), é um protocolo que faz a tradução dos endereços IP *(Internet Protocol*) e portas TCP (*Transmission Control Protocol*) da rede local para a Internet. Ou seja, o pacote enviado ou a ser recebido de sua estação de trabalho, vai até o servidor, onde é trocado pelo IP deste servidor. Em seguida, substitui o IP da rede local validando assim o envio do pacote na internet. O mesmo acontece no retorno do pacote; o pacote chega e o endereço IP do servidor é trocado pelo endereço IP da estação que fez a requisição do pacote. (AMADEU, 2004)

Delay Pools

Delay Pools é um recurso disponível no servidor proxy Squid capaz de fazer o controle de banda da internet.

Existem cinco *Delay Pools Class*, mas a classe 4 – que foi utilizada no projeto – existe apenas a partir da versão 3 do Squid e é utilizada para fazer controle de banda por usuários. (LUYER, 2009)

A classe 1 faz o controle de banda de toda rede. A classe 2 limita a banda por toda rede e por endereços de IP individual considerando apenas o último octeto. A classe 3 faz a mesma função da classe 2 mas também faz o controle através dos dois últimos octetos, o que a faz torna uma classe ideal para trabalhar com controle individual de IP. A classe 4 trabalha com logins de usuários e a classe 5 com tags (etiquetas). (ERIBERTO, 2011)

MÉTODOS

Para o desenvolvimento do projeto foi utilizado um computador com processador core i3 com 4gb de memória RAM e 1TB de disco rígido com o sistema operacional Windows 7 e com velocidade de acesso à internet de 15Mpbs.

Foi instalado o programa VMWare para a virtualização das máquinas.

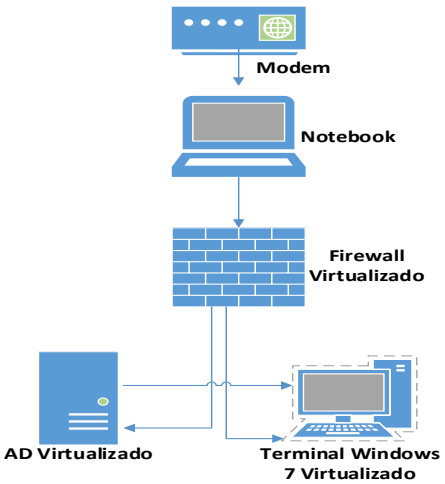
Na primeira máquina com VMWare foi instalado o sistema operacional Windows Server 2008 R2, e neste, instalou-se os serviços de AD (*Active Directory*).

Na segunda máquina foi instalado o sistema operacional Ubuntu Server 14.04 com os serviços de Squid3, Bind9 onde foram configurados os DNS do servidor e o dhcp-server.

Na terceira máquina foi instalado um Windows 7 apenas para testes.

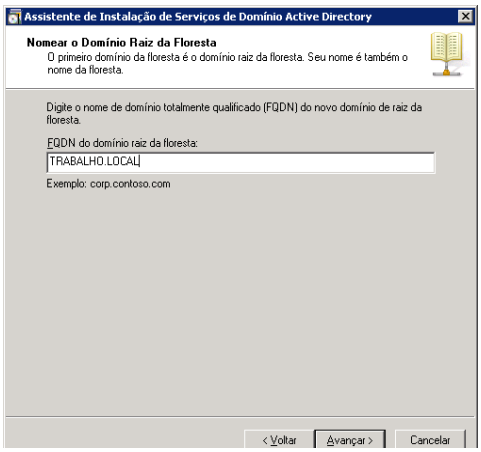
A Figura 1 apresenta a topologia de rede utilizada para criação do projeto.

Figura 1: Topologia de rede



Na máquina com Windows Server, foi instalado o serviço de Domínio de Active Directory e através do DCPROMO.exe, foi criado uma nova floresta – domínio criado dentro do AD para identificação e autenticação com o AD – com nome de TRABALHO.LOCAL como exibido na Figura 2. A floresta foi criada com nível de Windows Server 2008 R2.

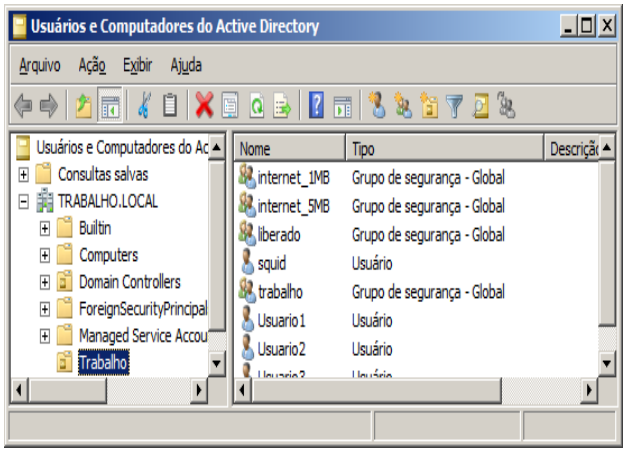
Figura 2: Criação da floresta do AD.



Assim que se inicia a criação da floresta, o Windows solicita para que seja instalado também o serviço de DNS (*Domain Name Server* – servidor de nomes do domínio) do Windows Server.

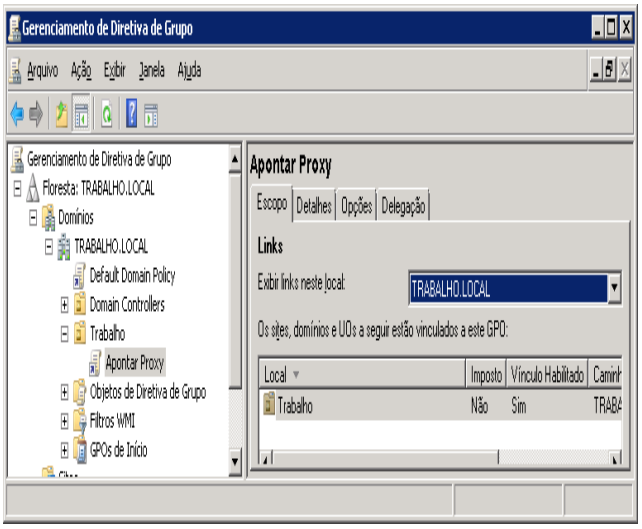
Após a instalação do serviço de AD, como mostra a Figura 3, foram criados quatro grupos de trabalho: internet_1MB, internet_5MB, liberados e o grupo trabalho onde foram colocados todos os grupos e usuários. Também foram criados os usuários: Usuario1 no grupo internet_1MB, Usuario2 no grupo internet_5MB, Usuario3 no grupo liberado e o usuário Squid para a autenticação do Squid com o AD.

Figura 3: Usuários e Grupos do AD.



Foi criada uma GPO (*Group Policy*) para que todas as máquinas do domínio utilizem Proxy na porta padrão do Squid – porta 3128, impossibilitando o usuário alterar o Proxy (Figura 4).

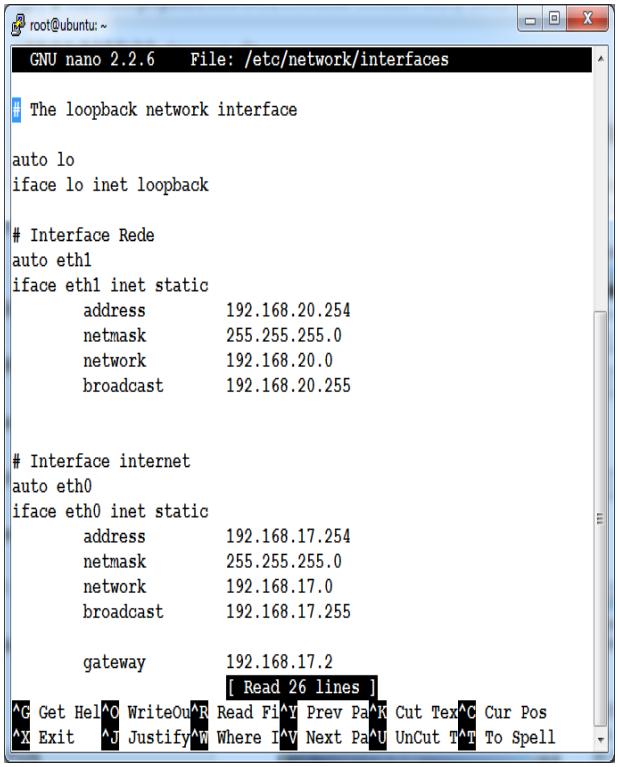
Figura 4**:** GPO criada para apontar Proxy.



Para a edição de todos os arquivos no Linux foi utilizado o editor de texto nativo do Linux o NANO por ser um editor simples e eficiente.

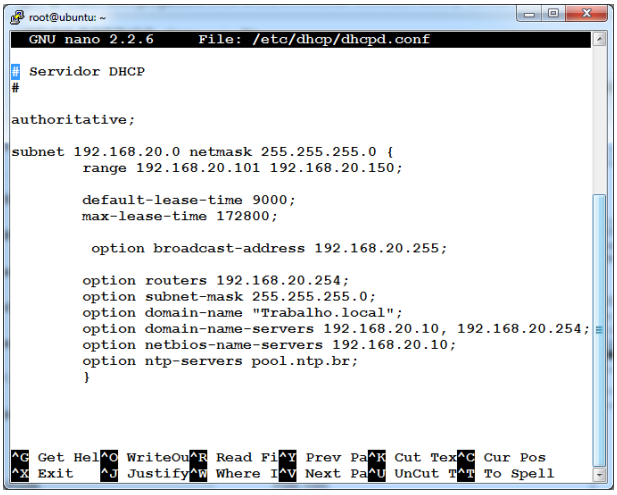
Na Figura 5, é apresentada a configuração do IP fixo dentro do arquivo /etc/network/interfaces.

Figura 5: Arquivo Interfaces com os Ips configurados



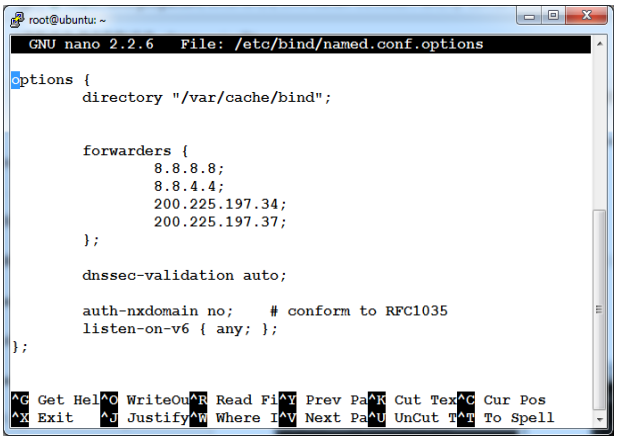
A Figura 6 apresenta como é configurado o servidor DHCP no qual definimos a faixa de endereços que será atribuída aos clientes na rede, gateway, DNS, NTP (*Network Time Protocol*) editando-se o arquivo de configuração /etc/dhcp/dhcpd.conf.

Figura 6: Arquivo de configuração do DHCP.



A Figura 7 apresenta a configuração do bind9 através da edição do arquivo de configuração /etc/bind/named.conf.options com os endereços dos servidores de DNS utilizados pelo servidor Linux.

Figura 7: Arquivo do Bind de configuração de DNS do Linux.



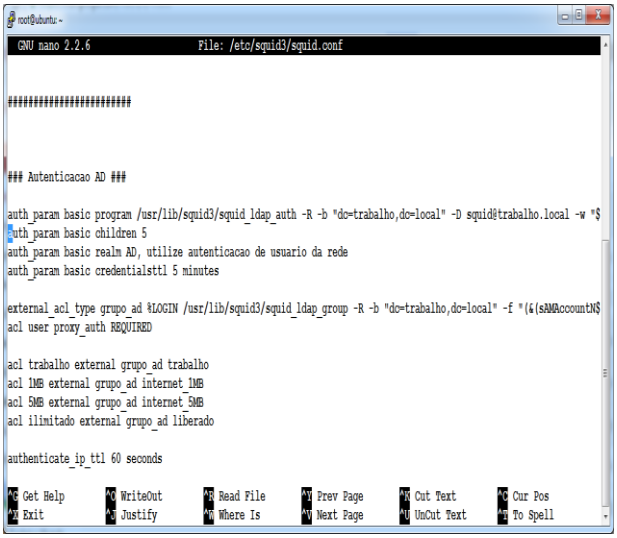
Para a instalação do Squid, necessitou-se trabalhar com os códigos fontes, realizando sua compilação. Foi preciso ativar todos os novos recursos do software Squid entre eles o novo *Delay Pools* que conta com as novas classes que trabalham por usuários.

Como apresenta a Figura 8, foi configurada a autenticação com o AD pelo arquivo do Squid3 /etc/squid3/squid.conf e também através do LDAP (*Lightweight Directory Access Protocol*) para onde foram carregados os grupos de trabalho do AD para o Squid3 onde conseguiremos controlar a velocidade da internet com o *Delay Pool*.

Com o LDAP, foram criadas três ACLs no Squid carregando os grupos de trabalho Internet1MB para a ACL

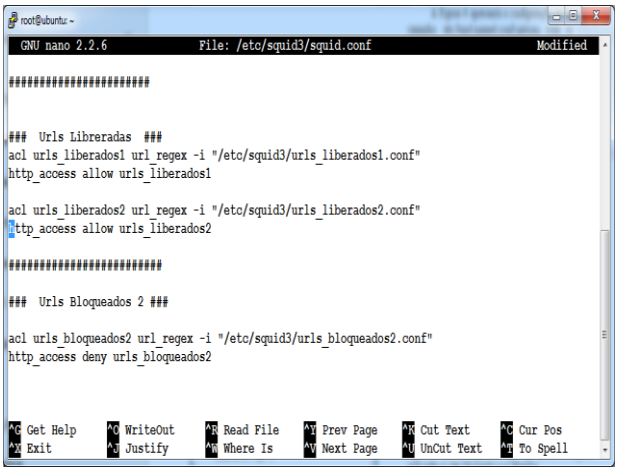
1Mbps, Internet5MB para a ACL 5Mbps e liberado para a ACL ilimitado, como apresentada na Figura 8.

Figura 8: Parte do arquivo do Squid que mostra a autenticação com o AD e a criação das ACLs onde serão guardados os grupos do AD.



Ainda dentro do arquivo squid.conf, foi configurado o arquivo com sites bloqueados e os sites liberados conforme política de segurança definida, carregados a partir dos arquivos urls_liberados1.conf, urls_liberados2.conf e urls_bloqueados2.conf como apresentado na figura 9.

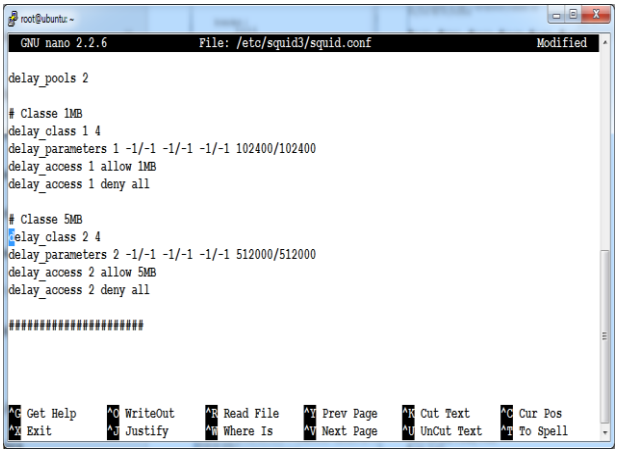
Figura 9: Parte do arquivo do Squid que mostra os arquivos onde estão os sites bloqueados e os liberados.



A Figura 10 demonstra a configuração do Delay Pool onde o grupo internet_1MB foi limitado a 1Mbps e o internet_5MB limitado a 5Mbps. Foi utilizado o delay_class 4 por ser a classe ideal para se controlar banda por usuários.

O delay pools trabalha com medidas de taxa de envio/recepção em bytes. Para limitar a banda em 1Mbps, por exemplo, basta colocar quantidade total de 1024000 bytes no *delay_parameters.*

Figura 10: Parte do arquivo do Squid que mostra o controle de banda feita pelo o Delay Pools.

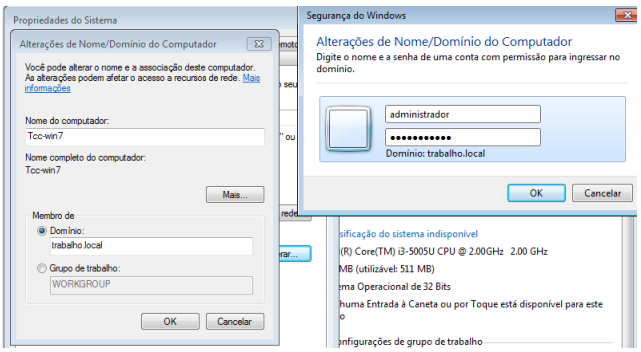


Também foi criada uma regra IPTables para fazer o NAT(*Network Address Translate*), e redirecionar o tráfego da porta 80 para a 3128 e bloquear sites com HTTPS que utilizam a porta 443 como, por exemplo, youtube, facebook entre outros, e salvo no arquivo /etc/firewall/firewall.sh e outro no arquivo /etc/firewall/Proxy.sh. Sendo criados arquivos de configuração do firewall para URLs liberadas no arquivo /etc/firewall/url_liberadas.conf e URLs bloqueadas no arquivo /etc/firewall/url_bloqueados.conf . Os computadores do domínio não precisam desse procedimento, pois a GPO criada no AD aponta o Proxy automaticamente para a porta 3128, mas os demais equipamentos fora do domínio, como celulares ou notebooks, serão bloqueados além dos sites HTTP que utiliza a porta 80 e os sites com HTTPS.

Ainda no servidor Linux foi preciso configurar o arquivo hosts no arquivo /etc/hosts apontando o nome do servidor AD com o IP do servidor AD.

A Figura 11 exibe o procedimento para colocar a máquina com Windows 7 no domínio. Instalou-se o navegador Chrome para testes.

Figura 11:Colocando a máquina com Windows 7 no domínio.

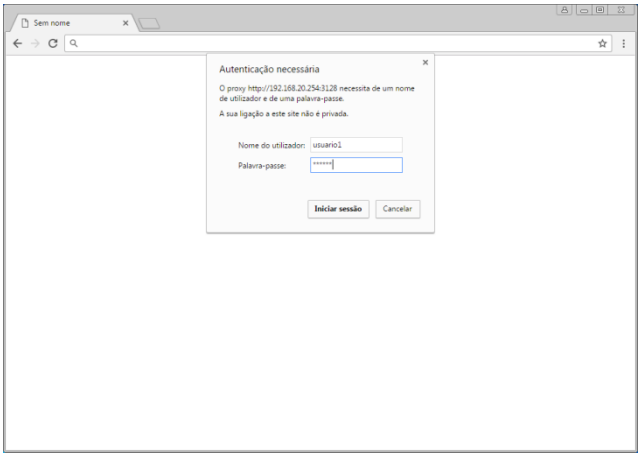


Todos os testes de velocidade de internet foram realizados no site fast.com, por se tratar de um velocímetro simples que mostra apenas a velocidade de download.

RESULTADOS E DISCUSSÃO

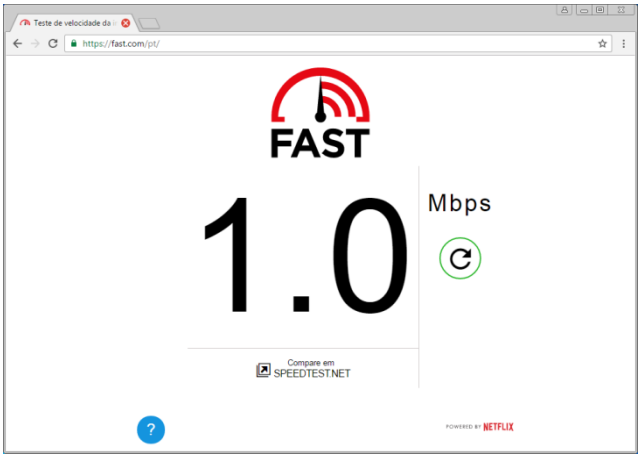
Com o intuito de verificar os resultados obtidos, foram realizados vários testes. Sempre que o usuário inicializasse seu navegador, foram requeridos usuário e senha para prosseguir com a navegação, como apresenta a Figura 12. Qualquer programa que utilizasse a internet para funcionar, pediria também usuário e senha para que o usuário só tivesse acesso com a sua identificação.

Figura 12: Solicitação de senha ao abrir o navegador.



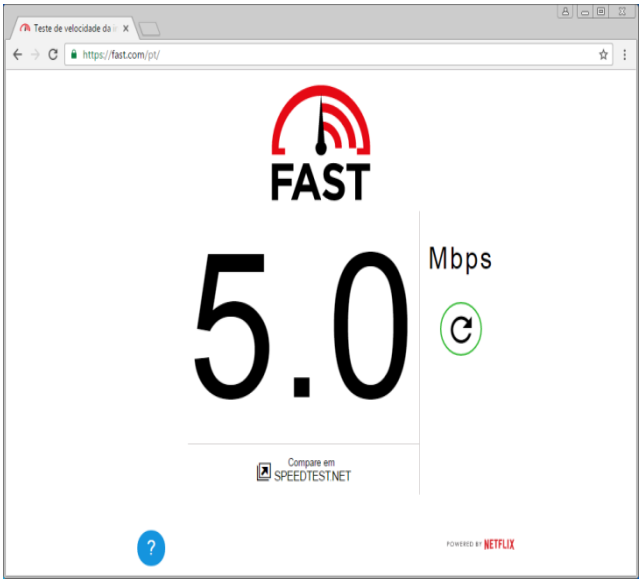
A Figura 13 apresenta a velocidade registrada para o usuario1 que está dentro do grupo do AD Internet_1MB e, portanto, limitado a 1 Mbps.

Figura 13: Tela de velocidade registrada pelo usuario1.



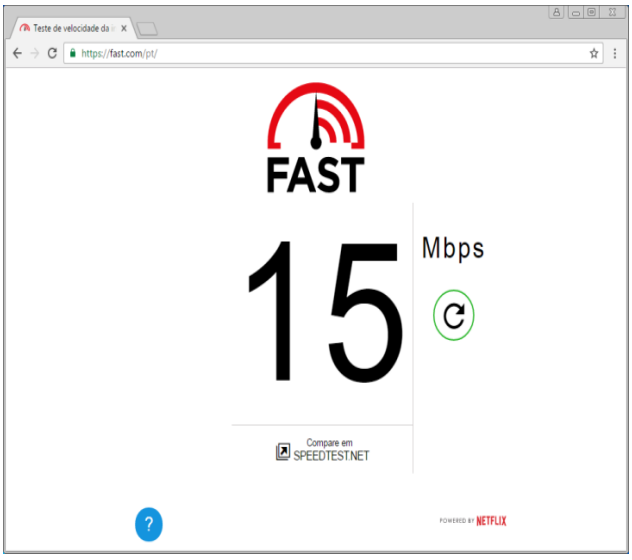
A Figura 14 identifica que a velocidade registrada para o usuario2 foi de 5 Mbps, pois foi o limite estabelecido para o grupo Internet_5MB.

Figura 14: Tela de velocidade registrada pelo usuario2.



A Figura 15 apresenta a velocidade registrada para o usuario3. Velocidade registrada para o usuario3 que está dentro do grupo Liberados e não possui limitação de banda.

Figura 15: Tela de velocidade registrada pelo usuário3.



Como se mostra no Quadro 1 foi comparada a velocidade de download e a velocidade efetiva de quando se baixa um arquivo entre os grupos do AD. A diferença entre a velocidade de download efetiva do grupo limitado a 1 Mbps e o grupo sem limite é muito alta. Portanto, um download sem o controle devido poderia atrapalhar todo o tráfego da rede.

Quadro 1: Quadro comparativo entre a velocidade de download dos grupos do AD.

Grupo do AD	Vel. configurada	Vel. Recebida.	Vel. efetiva
1MB	1 Mb/s	0,9 Mbps a 1,2 Mbps	1220 Kbps
5MB	5 Mb/s	4,99 Mbps a 5,1 Mbps	5400 Kbps
Liberado	15 Mb/s	14,5 Mbps a 15 Mbps	16400 Kbps

A escolha da utilização do Squid, utilizando *Delay Pools* para o controle de banda, se deu com a possibilidade de integração de um Squid com o AD, e com isso o controle de banda por usuários.

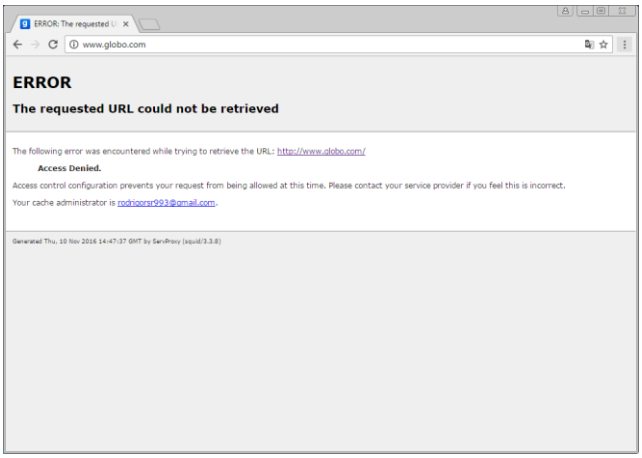
Como exibido na Quadro 2. O Squid consegue fazer um controle por usuários e outras ferramentas não conseguem.

Quadro 2: Quadro comparativo de alguns programas de controle de banda e como trabalham.

Ferramentas	Tipo de controle de banda
WebHTB	IP - MAC
Roteadores Wireless	IP - MAC
Switchs Gerenciáveis	IP - MAC - Porta
Squid (Delay Pools)	IP - MAC – Usuários

Os usuários dos grupos Internet_1MB e Internet_5MB também têm uma lista de sites bloqueados e sempre quando acessam um site que não tem permissão, é apresentada uma página de bloqueio como apresenta a Figura 16.

Figura 16: Página de bloqueio quando o usuário não tem acesso à página solicitada.



CONCLUSÃO

Uma grande vantagem na limitação e controle por grupos de usuários é de que não importa qual o computador o usuário utilize dentro da empresa, ele sempre vai ser limitado e bloqueado conforme a regra para seu grupo.

A aplicação do projeto apresentado neste artigo, mostrou como é eficiente o controle de banda utilizando a integração com um AD e um Proxy Squid. Os resultados foram satisfatórios. Uma rede bem administrada dificilmente vai passar por problemas provocados por mau uso de banda.

REFERENCIAS

AMADEU. R. **Afinal, o que é NAT?** Disponível em: <http://imasters.com.br/artigo/1904/redes-e-servidores/afinal-o-que-e-nat/?trace=1519021197&source=single >. Acesso em 01/11/2016.

AUGUSTO. F. **Criando delay pools (Proxy/Squid).** Disponível em: <https://www.vivaolinux.com.br/artigo/Criando-delay-pools-(Proxy-Squid)>. Acesso em 01/10/2016.

BRANDÃO. R. **Introdução a Group Policy(GPO).** Disponível em: <https://technet.microsoft.com/pt-br/library/cc668545.aspx >. Acesso em 19/11/2016.

BUCKMINSTER. B. **Copilando o Squid3.** Disponível em: <https://www.vivaolinux.com.br/artigo/Compilando-o-Squid3 >. Acesso em 01/11/2016.

ERIBERTO. J. **Implementação de delay pools com Squid.** Disponível em: < https://eriberto.pro.br/wiki/index.php?title=Implementa%C

3%A7%C3%A3o_de_delay_pool_com_Squid>. Acesso em 15/10/2016.

ERICH. S. **Autenticação Integrada Baseada em Serviço de Diretório LDAP.** Disponível em: <http://www.linux.ime.usp.br/~cef/mac499-

06/monografias/erich/html/ch01s05.html>. Acesso em 15/10/2016.

FBNEWSROOM. **State of Connectivity 2015: A Report on Global Internet Access.** Disponível em: <http://newsroom.fb.com/news/2016/02/state-of-connectivity-2015-a-report-on-global-internet-access/ >. Acesso em 19/11/2016.

GARCIA. R. **Utilizando Delay_Class 4 do SQUID 3 Integrado ao AD.** Disponível em: <https://www.vivaolinux.com.br/dica/Utilizando-delay-class-4-do-Squid-3-Integrado-ao-AD>. Acesso em 01/10/2016.

LUYER. D. **Feature: Delay Pools.** Disponível em: <http://wiki.squid-cache.org/Features/DelayPools >. Acesso em 19/11/2016.

MACHADO. C. SOARES. D. REY. L. CERON. J. JÚNIOR. A. **Implantação do Sistema de Registro de Estações da UFRGS.** Disponível em: <http://www.lume.ufrgs.br/bitstream/handle/10183/16098/000697616.pdf?sequence=1 >. Acesso em 19/11/2016.

MACIEL. R. B. **Protótipo de Aplicação WEB para Gerenciamento de Firewall Linux.** Disponível em: <http://dsc.inf.furb.br/arquivos/tccs/monografias/2005-2regismacielborscheidvf.pdf>. Acesso em 01/10/2016.

MARCELO. A. **SQUID.** Rio de Janeiro: Abreu System, 2006. p.3-8.

MELLO. J. **Descomplicando Passo a Passo GPO e Active Directory.** Aracaju: Clube dos Autores, 2014. p.4-5

MENEZES, D. F. **Virtualização: VMWare e Xen**. Disponível em: <http://recreio.gta.ufrj.br/grad/08_1/virtual/artigo.pdf >. Acesso em 10/10/2016.

MOSHARRAF. F. , FOROUZAN. B. **Rede de computadores uma abordagem TOP-DOWN.** Porto Alegre: AMGH, 2013. p.21-22

MUNIZ. V. **O que é IPTables, para que serve, como usar?** Disponível em: <http://viniciusmuniz.com/o-que-e-iptables-para-que-server-como-usar/ >. Acesso em 20/11/2016.

SANTOS, M. **Uso de LDAP Implementado em Software Livre Para Integrar a Autenticação dos Controladores de Domínio MS-ACTIVE DIRECTORY E SAMBA/LINUX.** Disponível em: <http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/2377/1/MD_COADS_2013_1_07.pdf >. Acesso em 20/09/2016.

TRIGO.C.H. OpenLDAP - **Uma Abordagem Integrada.** São Paulo: Novatec, 2007. p.239.

VMWARE. **Choose Cloud Infrastructure and Business Mobility Solutions Enabled by VMware Innovation?** Disponível em: < http://www.vmware.com / >. Acesso em 01/11/2016.