FACULDADE DE TECNOLOGIA
SENAC PELOTAS

Curso Superior em Tecnologia de Redes de Computadores

Projeto Integrador II

2º Seminário de Andamento

Jones Bunilha Radtke
jones.radtke@gmail.com

FACULDADE DE TECNOLOGIA
SENAC PELOTAS

Solução em *Software* Livre para Controle de Acesso a Conteúdo *Web*

Jones Bunilha Radtke
jones.radtke@gmail.com

Sumário

- Introdução
- Objetivos
  - Geral
  - Específicos
- Projeto
  - Situação atual
  - Próximos passos
- Cronograma
- Referências Bibliográficas

Introdução

Todas redes de computadores que possui uma administração, se faz necessário:

- Controle e o monitoramento sobre o conteúdo *Web;*
  - Segurança;
  - Qualidade de acesso a serviços;
- Produtividade;
- Flexibilidade para utilização da rede;
- Fácil administração.

Objetivos

Objetivo Geral

- Pesquisar e apresentar uma solução em *software* livre que possibilite o controle de acesso a conteúdo Web com autenticação automática de usuário.

Objetivos Específicos

- Pesquisar soluções de Proxy que possibilite autenticação dos usuários;
- Pesquisar mecanismos de integração do Proxy com o Active Directory;
- Testar e analisar as ferramentas pesquisadas;
- Documentar todo processo de pesquisa e testes efetuado.

Projeto

Integração das ferramentas:

- **Squid**

Proxy cache para a Web com suporte a HTTP, HTTPS e FTP.

- **Active Directory Microsoft Windows**

Serviço de diretório da Microsoft.

- **Samba 4**

Implementação em *software* livre para o AD Microsoft Windows.

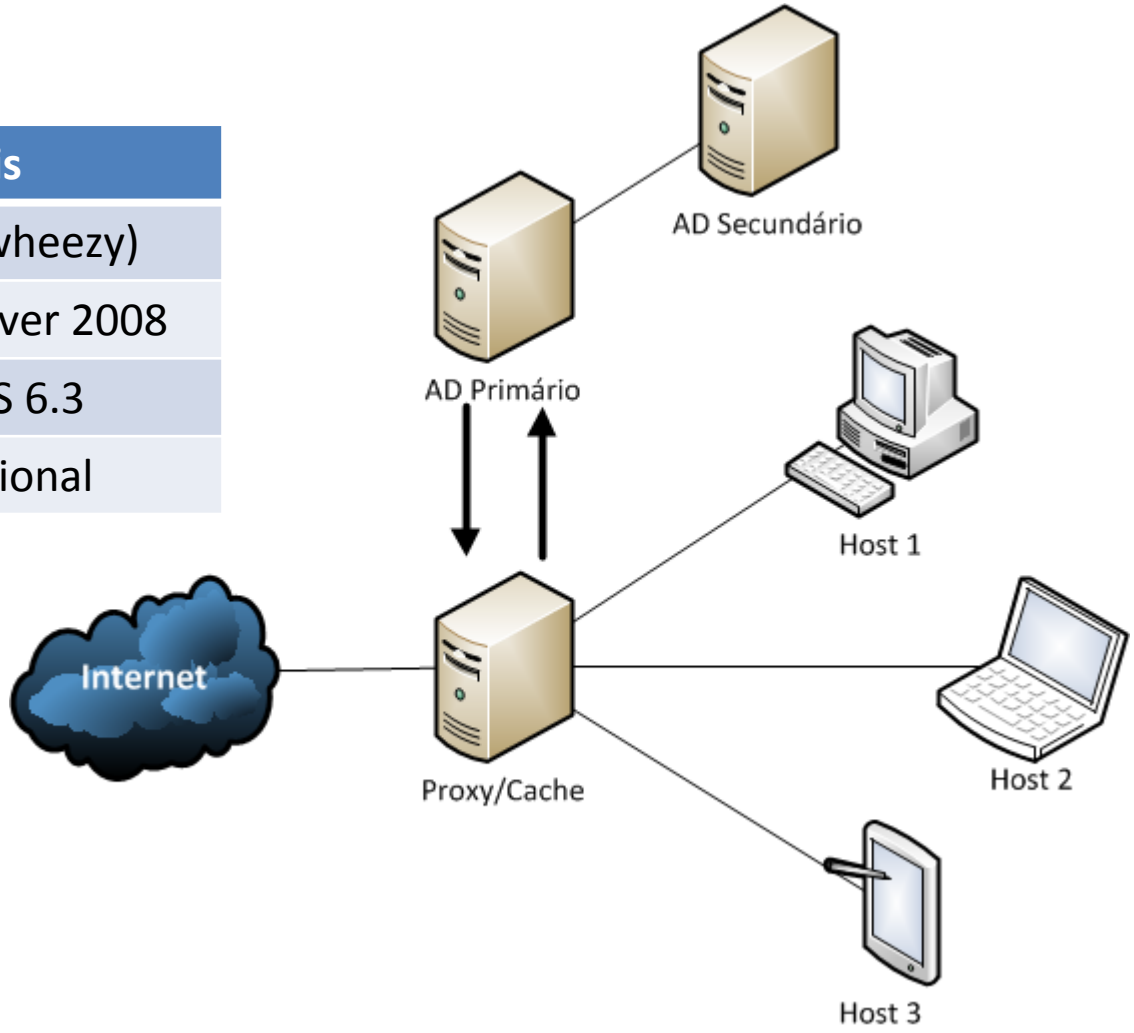
- **SARG**

Utilitário para geração de relatórios baseado no log do Squid.

Projeto

Cenário:

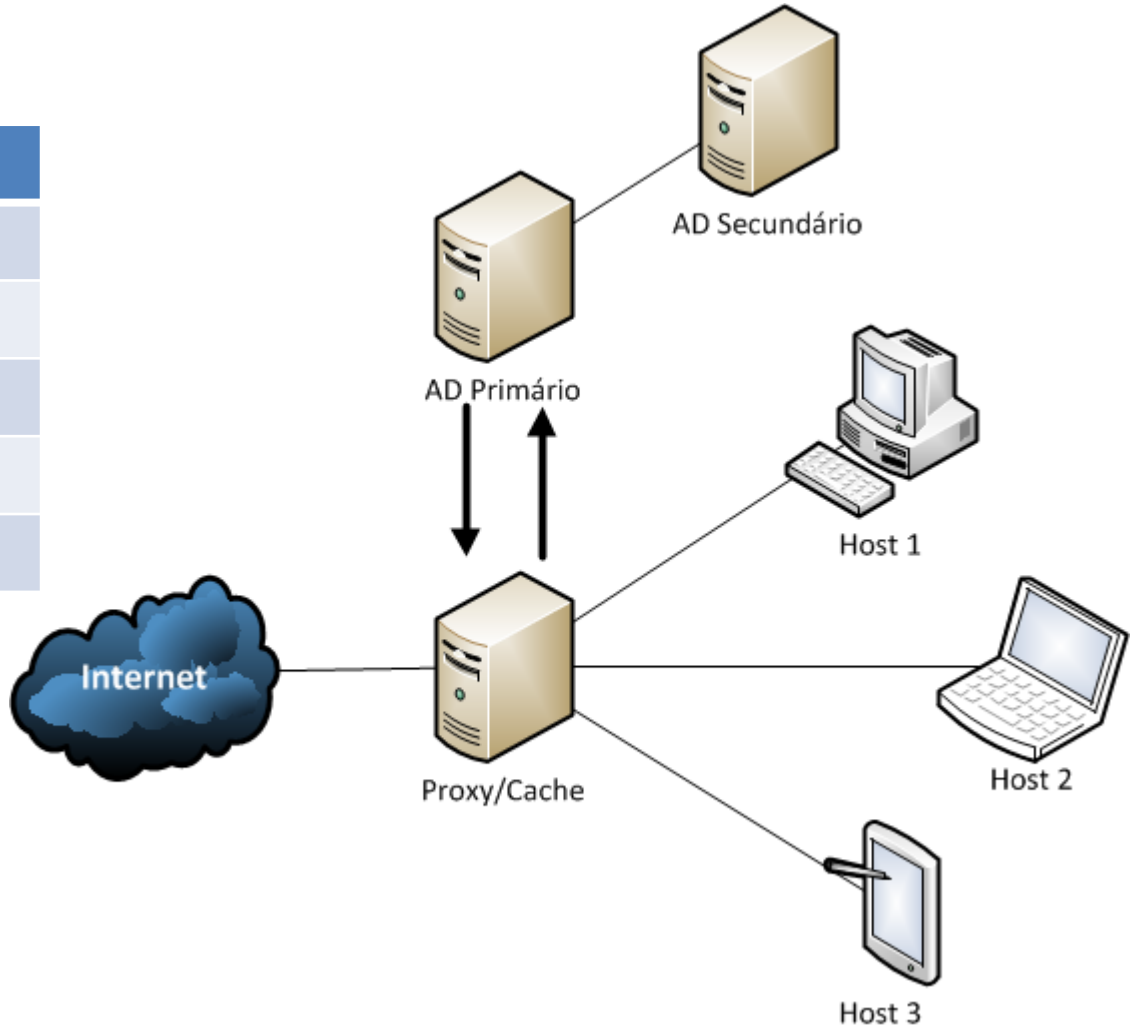
Sistemas Operacionais
Proxy/cache – Debian 7.4 (wheezy)
A.D. Primário – Windows server 2008
A.D. Secundário – CentOS 6.3
Host – Windows 7 Profissional



Projeto

Cenário:

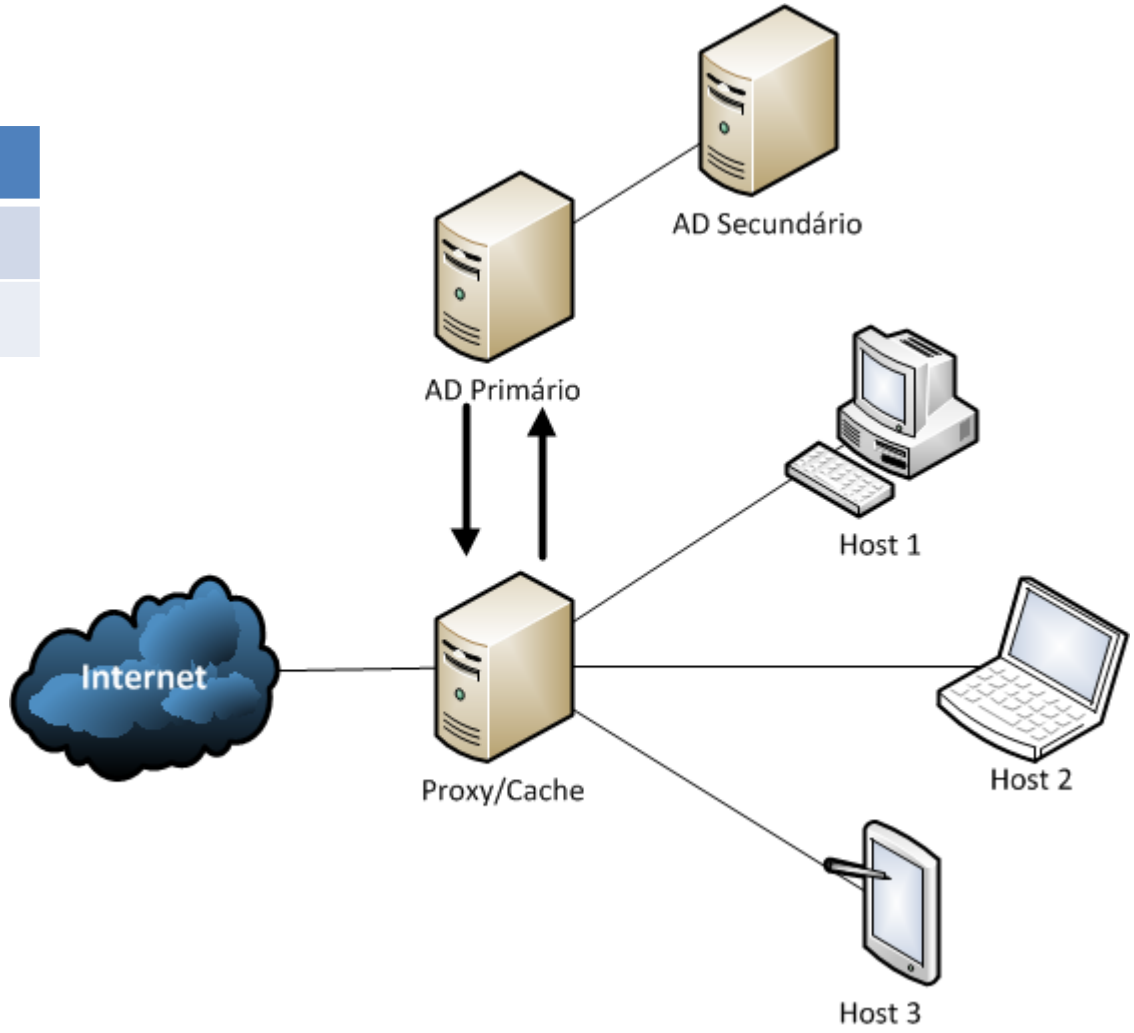
Utilitários Proxy/Cache
Squid 3
SARG
Kerberos (RFC 3244)
Samba
Winbind



Projeto

Cenário:

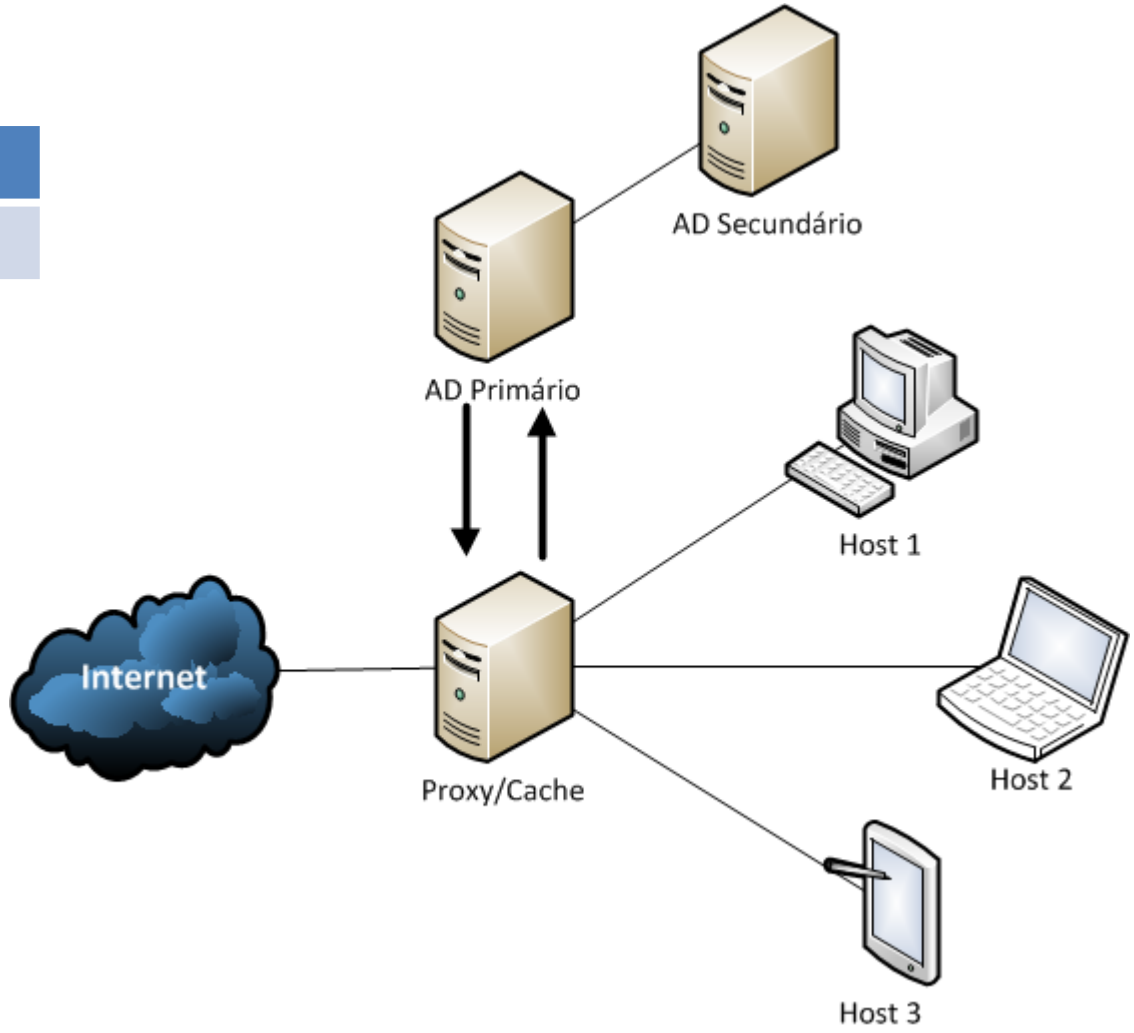
Utilitários AD Primário
Active Directory
DNS



Projeto

Cenário:

Utilitários AD Secundário
Samba 4

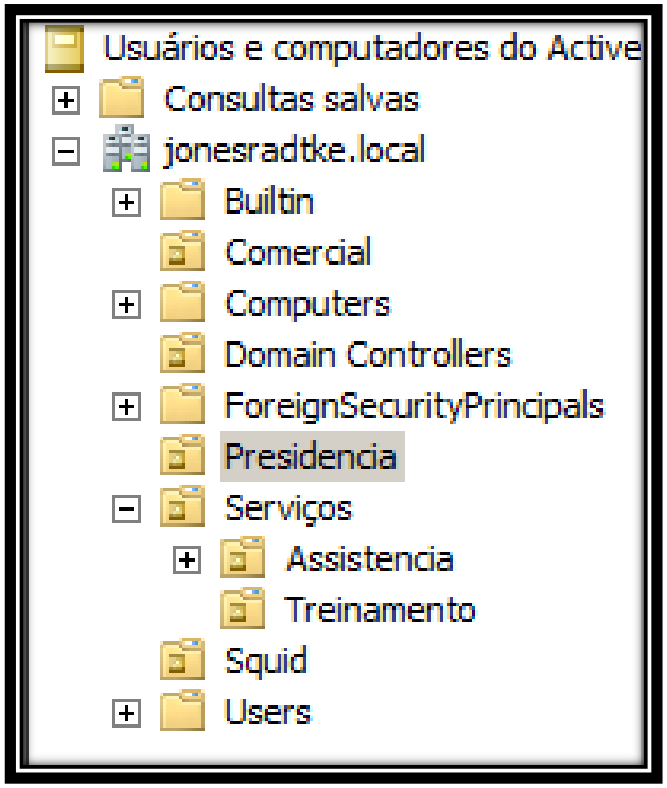


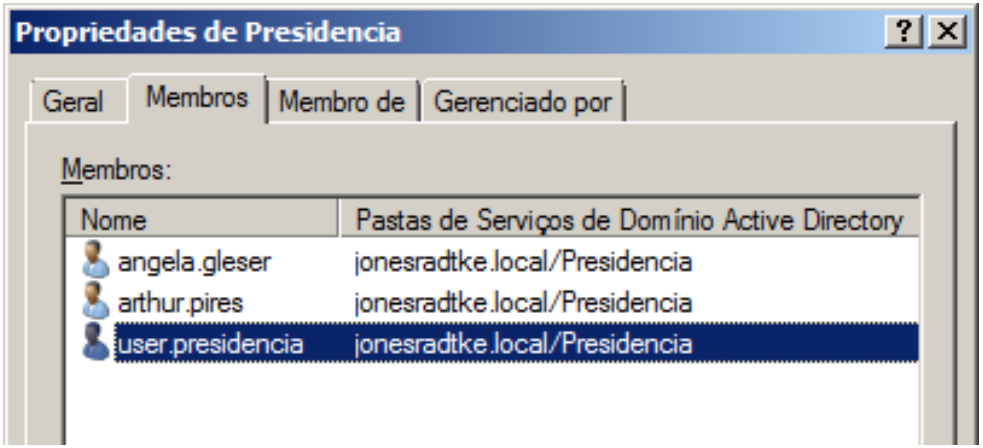
Projeto

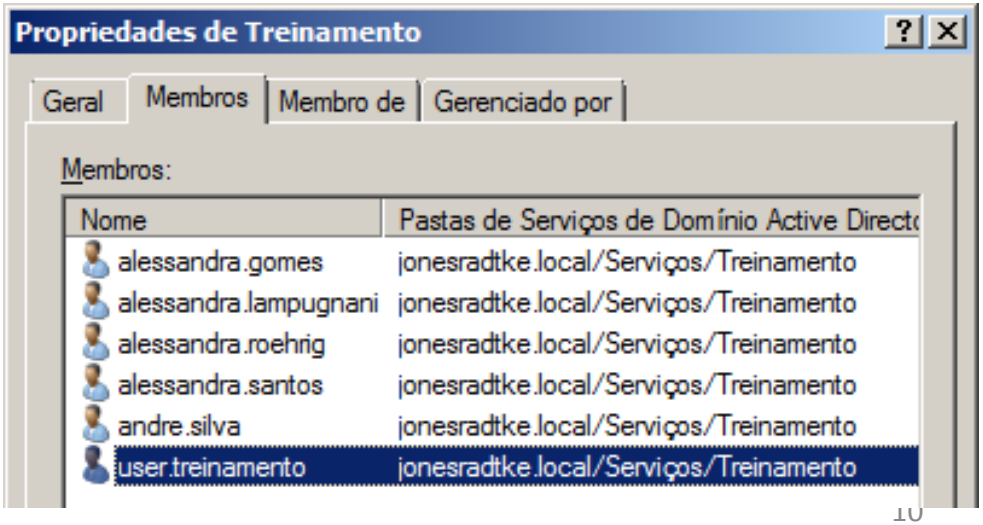
Servidores de Domínio - Estrutura do A.D.

VANTAGEM

Proxy Administrado pelo AD







Projeto

Servidor Proxy/Cache - Configuração do Squid

VANTAGEM

ACLs aplicadas por grupo de usuários

- **Arquivo /etc/squid3/squid.conf**

Módulos de autenticação.###########
auth_param ntlm program /usr/bin/ntlm_auth --helper-protocol=squid-2.5-ntlmssp
auth_param ntlm children 10
auth_param ntlm keep_alive on
auth_param basic program /usr/bin/ntlm_auth --helper-protocol=squid-2.5-basic

external_acl_type grupo_ad %LOGIN /usr/lib/squid3/wbinfo_group.pl

ACLs de grupos do A.D.###########
*acl **grp-presidencia** external grupo_ad **Presidencia***
*acl **grp-treinamento** external grupo_ad **Treinamento***

Permissões de acesso
*http_access allow **grp-presidencia** youtube*
*http_access deny **grp-treinamento** youtube*

Projeto

Squid Analysis Report Generator

VANTAGEM

Relatórios de acesso por usuário

Squid User Access Reports

Period: 2014 Jun 01

Sort: bytes, reverse

Top users

Top sites

Sites & Users

Denied accesses

Authentication Failures

NUM		USERID	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILLISEC	%TIME
1		user.presidencia	167	3.91M	87.04%	0.01%	99.99%	00:57:40	3,460,506	51.64%
2		jones.radtke	15	343.20K	7.63%	0.00%	100.00%	00:53:10	3,190,525	47.61%
3		172.16.0.3	35	118.91K	2.65%	100.00%	0.00%	00:00:00	200	0.00%
4		172.16.0.20	3	67.22K	1.50%	0.00%	100.00%	00:00:13	13,361	0.20%
5		172.16.0.22	4	43.21K	0.96%	0.00%	100.00%	00:00:13	13,443	0.20%
6		user.treinamento	8	9.82K	0.22%	88.76%	11.24%	00:00:23	23,624	0.35%
		TOTAL	**232**	**4.49M**		**2.85%**	**97.15%**	**01:51:41**	**6,701,659**	
		AVERAGE	**38**	**749.20K**				**00:18:36**	**1,116,943**	

Generated by sarg-2.3.2 Nov-23-2011 on Jun/01/2014 23:27

Projeto

Squid Analysis Report Generator

Squid User Access Reports

Period: 2014 Jun 01
User: user.presidencia
Sort: bytes, reverse
User report

ACCESSED SITE	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILLISEC	%TIME
r10---sn-hp576n7y.googlevideo.com	24	1.69M	43.29%	0.00%	100.00%	00:00:52	52,180	1.51%
s.ytimg.com	27	1.23M	31.51%	0.00%	100.00%	00:01:36	96,432	2.79%
i1.ytimg.com	29	297.95K	7.61%	0.10%	99.90%	00:01:10	70,287	2.03%
r19---sn-hp576nee.googlevideo.com	6	266.98K	6.82%	0.00%	100.00%	00:00:21	21,770	0.63%
www.youtube.com	12	125.06K	3.20%	0.00%	100.00%	00:00:18	18,071	0.52%
ssl.gstatic.com:443	2	55.87K	1.43%	0.00%	100.00%	00:08:13	493,141	14.25%
www.google.com	3	47.93K	1.23%	0.00%	100.00%	00:00:09	9,042	0.26%
oauth.googleusercontent.com:443	2	47.46K	1.21%	0.00%	100.00%	00:06:03	363,401	10.50%
apis.google.com:443	3	43.62K	1.11%	0.00%	100.00%	00:06:16	376,873	10.89%

Projeto

Squid Analysis Report Generator

Squid User Access Reports

Period: 2014 Jun 01
User: user.treinamento
Sort: bytes, reverse
User report

ACCESSED SITE	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILLISEC	%TIME	
www.youtube.com	2	8.72K	88.76%	100.00%	0.00%	00:00:00	26	0.11%	DENIED
vchwiwevjq	1	368	3.75%	0.00%	100.00%	00:00:00	90	0.38%	
tsfcwbiwskn	1	368	3.75%	0.00%	100.00%	00:00:00	107	0.45%	
lxwlplt	1	368	3.75%	0.00%	100.00%	00:00:00	83	0.35%	
www.google.com.br:443	3	0	0.00%	0.00%	0.00%	00:00:23	23,318	98.70%	
TOTAL	**8**	**9.82K**	**0.22%**	**88.76%**	**11.24%**	**00:00:23**	**23,624**	**0.35%**	
AVERAGE	**0**	**749.20K**				**00:18:36**	**1,116,943**	**16.67%**	

Generated by sarg-2.3.2 Nov-23-2011 on Jun/01/2014 23:27

Projeto

Passos anteriores:

- ~~Realizar a integração do Squid e DansGuardian;~~
- Cliente realizar a autenticação automática no Squid com usuário do AD; **OK**
- ~~Criar script de relatórios de acesso por usuário;~~
- Iniciar a escrita do artigo. **OK**

Projeto

Próximos Passos:

- Realizar testes de desempenho do proxy;
- Finalizar a escrita do artigo.

Cronograma

	Fev	Mar	Abr	Mai	Jun
Pesquisar soluções de *Proxy*	x	x	x		
Pesquisar mecanismos de integração do *Proxy* com o *Active Directory*	x	x	x	x	
Testar e analisar as ferramentas pesquisas			x	x	x
Documentar todo o processo		x	x	x	x

Referências Bibliográficas

- MORIMOTO, Carlos E. Servidores Linux, Guia Prático. Porto Alegre. GDH Press e Sul Editores, 2009.
- squid : Optimising Web Delivery. Acesso em 06 de março de 2014, disponível em http://www.squid-cache.org/;
- Samba - opening windows to a wider world. Acesso em 06 de março de 2014, disponível em https://www.samba.org;
- Introdução ao Active Directory. Acesso em 06 de março de 2014, disponível em http://technet.microsoft.com/pt-br/library/cc668412.aspx;
- DansGuardian. Acesso em 21 de abril de 2014, disponível em http://dansguardian.org/.

Wiki

Projeto Integrador II -2014-1 - Projeto 2

http://187.7.106.14/wiki2014_1/