

DOCUMENTAÇÃO TÉCNICA – PROJETO GSQUID

MANUAL COMPLETO DE INSTALAÇÃO, CONFIGURAÇÃO E UTILIZAÇÃO

AUTOR: Romulo Lobo

Sumário

BACKBONE.....	3
DOCUMENTAÇÃO TÉCNICA DA APLICAÇÃO GSQUID.....	6
INSTALAÇÃO.....	6
1º - Copiar a pasta da aplicação para um diretório no servidor.....	6
2º - Adicionar as permissões necessárias para o diretório e subdiretórios.....	6
3º - Criar a pasta mensagem no diretório root do servidor web.....	7
4º - Crie a pasta base para as ACLs do squid e aplique as permissões.....	7
5º - Configurar o arquivo sudoers para permitir que o usuário do apache tenha permissão de acessar o executável do squid.....	7
6º - Desabilitar a rotação de logs do arquivo access.log.....	8
7º - Agendar no crontab a execução dos scripts de manipulação de log do squid.....	8
8º - Configurar e importar a estrutura do banco de dados da aplicação.....	10
9º - Configurar a aplicação.....	10
10º - Ativando configuração de dhcp.....	14
UTILIZAÇÃO.....	15
AUTENTICAÇÃO.....	15
DASHBOARD.....	15
HOSTS POR SALA.....	19
BLACKLIST.....	21
BLOQUEIOS.....	21
CADASTRO.....	22
USUÁRIOS.....	23
ESTATÍSTICAS.....	24

BACKBONE

ESPECIFICAÇÕES	
Modelo	Dell Poweredge R210
Memória RAM	16 GB de RAM, expansível até 32 GB
Processador	Processador Intel Xeon E3-1200
Disco rígido	2 HDs SATA II de 500 GB
Interfaces de rede	2 interfaces gigabiEthernt

PARTIÇÕES	
/	Sda1(?? - definir tamanho)
/boot	sda2(?? - definir tamanho)
/cache	sdb(500Gb)
/backups	Ipdeoutroservidor:3:home/backups/(?? - definir tamanho)

CONFIGURAÇÕES DE REDE (Utilizar Ips conforme realidade local)	
Interface em1	10.10.0.1 /16
Interface em2	192.168.25.? /24
DNS 1	8.8.8.8
DNS 2	8.8.4.4
Gateway	192.168.25.1

SERVIÇOS CONFIGURADOS	
SERVIÇO	DESCRIÇÃO
SSH	Credenciais: <ul style="list-style-type: none">• root: senha
NTP	<ul style="list-style-type: none">• Sincronizado com servidores brasileiros• Utilizado como referência de horário
DNS	Domínio(endereços de exemplo) <ul style="list-style-type: none">• mpie.br IN A 10.10.0.1 (backbone) Subdomínios <ul style="list-style-type: none">• proxy.mpie.br IN A 10.10.0.1 (backbone)• zabbix.mpie.br IN A 10.10.0.3 (gerencia)

HTTP	<p>Aplicação Gsquad</p> <ul style="list-style-type: none"> • Diretório raiz: /var/www/squid • Domínio: proxy.mpie.br • Domínio: proxy.mpie.br • Utilização de certificado digital (RSA 2048 bits + SHA256) válido até 11/08/2043 • Acesso somente via protocolo TLSv1.2
MySQL	<p>Database da aplicação Gsquad</p> <ul style="list-style-type: none"> • Gsqui <p>Credenciais:</p> <ul style="list-style-type: none"> • Root:? • Mpie: ?
Squid	<p>Diretório de configuração:</p> <ul style="list-style-type: none"> • /etc/squid <p>Diretório de logs:</p> <ul style="list-style-type: none"> • /var/log/squid/
ufdbGuard	<p>Arquivo de configuração:</p> <ul style="list-style-type: none"> • /etc/ufdbguard/ufdbGuard.conf <p>Diretório de blacklists:</p> <ul style="list-style-type: none"> • /var/ufdbguard/blacklists/ <p>Blacklists:</p> <ul style="list-style-type: none"> • /var/ufdbguard/blacklists/porn/domains • /var/ufdbguard/blacklists/proxies/domains • /var/ufdbguard/blacklists/tor/domains <p>Unindo blacklists:</p> <ul style="list-style-type: none"> • cp /var/ufdbguard/blacklists/proxies/domains /tmp/ • cat blacklist_nova.txt >> /tmp/domains • cat /tmp/domains awk '!seen[\$0]++' > • /var/ufdbguard/blacklists/proxies/domains <p>Inserindo site na blacklist:</p> <ul style="list-style-type: none"> • echo "site.com" >> /var/ufdbguard/blacklists/proxies/domains <p>Atualizando blacklists:</p> <ul style="list-style-type: none"> • ufdbConvertDB /var/ufdbguard/blacklists/ • /etc/init.d/ufdb reconfig
Firewall	<p>Política proibitiva (INPUT e FORWARD)</p> <p>...</p>

Otimização para o squid

/etc/sysctl.conf	<pre>##### TUNNING PARA SQUID ##### # Reduzir o tempo de limpeza da tabela ARP</pre>
------------------	--

	<pre># Expandir o seu tamanho net.ipv4.neigh.default.gc_interval = 15 net.ipv4.neigh.default.gc_thresh1 = 4096 net.ipv4.neigh.default.gc_thresh2 = 8192 net.ipv4.neigh.default.gc_thresh3 = 16384 # Aumento do numero de conexoes simultaneas # Reducao do tempo de espera entre as conexoes net.core.somaxconn = 20480 net.core.netdev_max_backlog = 2048 net.ipv4.tcp_fin_timeout = 10 net.ipv4.tcp_tw_recycle = 1 net.ipv4.tcp_tw_reuse = 1 net.ipv4.tcp_syn_retries = 1 net.ipv4.tcp_synack_retries = 1 net.ipv4.tcp_max_syn_backlog = 2048</pre>
/etc/security/limits.conf	<pre>net.ipv4.tcp_max_syn_backlog = 2048 ####TUNNING DE LIMITS DE KERNEL#### root soft nfile 16384 root hard nfile 32768 * soft nfile 16384 * hard nfile 32768</pre>
/etc/init.d/squid	<pre>Ulimit -n 16384</pre>

DOCUMENTAÇÃO TÉCNICA DA APLICAÇÃO GSQUID

A seguir iniciam os processos de instalação e configurações iniciais da ferramenta Gsquad.

INSTALAÇÃO

Lista de serviços instalados (dependências):

- Httpd, httpd-tools, php, php-mysql, mysql, mysql-server, gd-devel, php-gd;
- Squid;
- Dhcp (opcional).

A seguir listamos os componentes da aplicação:

- Pasta da aplicação;
- Arquivo `*squid_senac.sql` contendo a estrutura do banco de dados. ***Nome a ser ajustado conforme determinação local!**
- Script do crontab;

- squidlog.sh

A seguir o passo a passo para instalação:

1º - Copiar a pasta da aplicação para um diretório no servidor

Este diretório pode ser o diretório root do servidor web ou um diretório personalizado. No caso de um diretório personalizado, será necessário realizar configurações avançadas no servidor web. O diretório root padrão do servidor web apache no CentOS fica localizado no seguinte diretório:

```
/var/www/html/
```

Nesse exemplo será utilizado o seguinte diretório:

```
/var/www/squid
```

2º - Adicionar as permissões necessárias para o diretório e subdiretórios

```
chown -R apache.apache /var/www/squid
```

```
chmod -R 755 /var/www/squid
```

```
chown -R squid.apache /var/log/squid
```

```
chmod -R 774 /var/log/squid
```

```
chmod -R 774 /var/www/squid/temp
```

```
chown
```

3º - Criar a pasta mensagem no diretório root do servidor web

Esta pasta será utilizada pela aplicação para criar dinamicamente páginas de bloqueio personalizadas para os usuários. Portanto, deve estar acessível para qualquer usuário.

```
mkdir /var/www/html/mensagens
```

```
chown -R apache.apache /var/www/html/mensagens
```

4º - Crie a pasta base para as ACLs do squid e aplique as permissões

A pasta “acls” conterà todos os arquivos de acls do squid.

As permissões do arquivo de configuração do squid deverão ser mudadas, pois a aplicação irá ler e gravar nesse arquivo com o usuário apache.

```
mkdir /etc/squid/acls
```

```
chown -R squid:apache /etc/squid/acls
```

```
chmod -R 775 /etc/squid/acls
```

```
chown squid:apache /etc/squid/squid.conf
```

```
chmod 775 /etc/squid/squid.conf
```

5º - Configurar o arquivo sudoers para permitir que o usuário do apache tenha permissão de acessar o executável do squid

Esta configuração é necessária para que o usuário apache possa reiniciar a configuração do squid para aplicar as configurações.

Para editar o arquivo sudoers digite:

```
vi /etc/sudoers
```

ou

```
vi sudo
```

Inserir nas últimas linhas as seguintes linhas:

```
Defaults !authenticate
```

```
apache ALL=NOPASSWD:/usr/sbin/squid
```

6º - Desabilitar a rotação de logs do arquivo access.log

Por padrão o squid vem configurado para realizar uma rotação de todos seus arquivos de log localizados no diretório /var/log/squid/. Deve-se desabilitar ou configurar para que o arquivo access.log não sofra rotação, deixando o log original para sempre.

No exemplo abaixo, somente o arquivo cache.log sofrerá rotação.

Editar o arquivo:

```
vi /etc/logrotate.d/squid
```

Alterar a seguinte linha:

```
/var/log/squid/*.log
```

Para:

```
/var/log/squid/cache.log
```

7º - Agendar no crontab a execução dos scripts de manipulação de log do squid

A pasta “scripts” contém o script “squidlog.sh”, que é responsável por organizar os logs de acesso do squid em turnos (madrugada, manhã, tarde e noite). Este script deve ser inserido no agendador de tarefas do Linux para ser executado no final de cada turno.

O caminho completo da pasta “temp” da aplicação deve ser alterado no script seguinte o formato exigido. O script utilizará esta pasta para guardar os logs de acessos divididos em turnos.

Conteúdo do script squidlog.sh:

```
#!/bin/bash

# Insere na variável “temp” o caminho completo da pasta temp da aplicação
temp='/var/www/squid/temp'
# Insere na variável “linhas” o número de linhas do arquivo de logs de acesso do squid
linhas=`wc -l /var/log/squid/access.log | awk -F ' ' '{ print $1 }`

# Insere na variável “data” a data atual no formato ANO-MÊS-DIA
data=`date +%Y`-`date +%m`-`date +%d`

# Insere na variável “hora” a hora atual
hora=`date +%H`

# Insere na variável “minuto” o minuto atual
minuto=`date +%M`

# Insere na variável “madrugada” o turno atual
if [ "$hora" -lt 6 -a "$hora" -ge 0 ]; then
turno='madrugada'
elif [ "$hora" -lt 12 -a "$hora" -gt 5 ]; then
turno='manha'
elif [ "$hora" -lt 18 -a "$hora" -gt 11 ]; then
turno='tarde'
elif [ "$hora" -le 23 -a "$hora" -gt 17 ]; then
turno='noite'
else
turno='indefinido'
fi

# Se o número de linhas for maior que 700000, o arquivo de log será dividido em partes.
# Essa limitação foi necessária, pois o PHP acaba utilizando memória em excesso (> 512MB).
# Será criado um arquivo na pasta temp da aplicação no seguinte formato: squidlog. ANO-
MÊS-DIA.TURNO
# Exemplos:
# /var/www/squid/temp/squidlog.2016-05-07.madrugada
# /var/www/squid/temp/squidlog.2016-05-07.manha
# /var/www/squid/temp/squidlog.2016-05-07.tarde
# /var/www/squid/temp/squidlog.2016-05-07.noite
```



```

if [ "$linhas" -gt 700000 ]; then
    `split -dl 700000 /var/log/squid/access.log "$temp"/squidlog.$data."$turno".`
else
    `cp /var/log/squid/access.log "$temp"/squidlog.$data."$turno"`
fi

# Altera o dono, grupo e permissões de todos arquivos da pasta temp da aplicação
chown apache.apache "$temp"/*
chmod 775 "$temp"/*

# Insere todo o conteúdo do log atual no arquivo access.log.original
# O arquivo access.log.original contém todos os logs originais
cat /var/log/squid/access.log >> /var/log/squid/access.log.original

# O arquivo de log atual é zerado
echo "" > /var/log/squid/access.log

```

No exemplo abaixo, a pasta “scripts” foi colocada na pasta do usuário root.

Para agendar tarefas no crontab, digite:

```
crontab -e
```

Insira as seguintes linhas no final do arquivo:

```
59 5 * * * /root/scripts/squidlog.sh
```

```
59 11 * * * /root/scripts/squidlog.sh
```

```
59 17 * * * /root/scripts/squidlog.sh
```

```
59 23 * * * /root/scripts/squidlog.sh
```

8º - Configurar e importar a estrutura do banco de dados da aplicação

O arquivo **squid_mpie.sql** contém a estrutura do banco.

No exemplo abaixo foi criada a database com o nome de **squid_mpie** e em seguida o usuário

mpie. Esses nomes podem ser alterados, recomenda-se a criação de nomes e senhas conforme a política de cada instituição.

```
mysql -u root -p
```

```
CREATE DATABASE squid_mpie;
```

```
CREATE USER mpie@localhost IDENTIFIED BY 'senha';
```

```
GRANT ALL ON squid_mpie.* TO mpie@localhost;
```

```
FLUSH PRIVILEGES;
```

```
quit;
```

```
mysql -u root -p squid_mpie < squid_mpie.sql
```

9º - Configurar a aplicação

Existem dois arquivos que devem ser alterados:

- **conexao.php** (configuração da conexão com banco de dados);
- **config.php** (configurações da aplicação).

/var/www/squid/includes/conexao.php

- **\$database**: nome da database criada anteriormente
- **\$usuarioBanco**: usuário criado no banco de dados anteriormente
- **\$senhaBanco**: senha cadastrada para o usuário do banco de dados anteriormente

```
1  <?php
2
3
4  class db {
5      private $conexao;
6      private $tipoBanco = "mysql";
7      private $host = "localhost";
8      private $database = "squid_senac";
9      private $usuarioBanco = "senac";
10     private $senhaBanco = "senha";
11     private $query;
12     private $dados;
13     private $resultado;
```

- **/var/www/squid/includes/config.php**
 - A primeira parte do arquivo contém variáveis necessárias para o funcionamento da aplicação:
 - **\$pastaTemp**: caminho completo da pasta “temp” da aplicação
 - **\$arquivo_squid**: caminho completo do arquivo de configuração do squid
 - **\$arquivo_log**: caminho completo do arquivo de log “access.log”
 - **\$range_ips_regex**: expressão regular para uma range específica de endereços IPs.

Utilize uma expressão regular de acordo com a range utilizada em sua rede privada.

Exemplos:

- 192.168.0.0 /24 => /192\168\0\.[0-9]{1,3}/
- 172.16.0.0 /16 => /172\16\.[0-9]{1,3}\.[0-9]{1,3}/
- 10.0.0.0 /8 => /10\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}/

A aplicação utilizará essa expressão regular para extrair os acessos ao proxy a partir do arquivo “**access.log**”

- **\$acls_pasta**: caminho completo da pasta acls, onde conterà os arquivos de acl do squid
- **\$mensagens_pasta**: caminho completo da pasta mensagens, onde conterà as páginas web de mensagens para os usuários
- **\$mensagens_url**: URL que aponta para pasta mensagens, utilizada para redirecionar o usuário para as mensagens

```

1  <?php
2  /***** Variáveis para configurar o squid *****/
3  $pastaTemp = "/var/www/squid/temp/";
4  $arquivo_squid = "/etc/squid/squid.conf";
5  $arquivo_log = "/var/log/squid/access.log";
6  $range_ips_regex = "/10\10\.[0-9]{1,3}\.[0-9]{1,3}/";
7  $acls_pasta = "/etc/squid/acls/";
8  $mensagens_pasta = "/var/www/html/mensagens/";
9  $mensagens_url = "http://proxy.senacinformatica.br/mensagens/";
10

```

- A segunda parte do arquivo contém o início da configuração do arquivo **squid.conf** (arquivo de configuração do squid). As primeiras linhas do arquivo **squid.conf** são inseridas dentro do **array \$default[]**. Modifique de acordo a necessidade, em caso de dúvidas sobre a configuração do squid, consulte: <http://wiki.squid-cache.org/>

```

11  /***** Configuração default do squid *****/
12  $default[] = "# SQUID 3.1.23 ARQUIVO DE CONFIGURAÇÃO";
13  $default[] = "# BY - Senac informatica";
14  $default[] = "# Email: gfbalestrin@hotmail.com";
15
16  $default[] = "##### CONFIGURAÇÃO DEFAULT #####";
17  $default[] = "http_port 3128";
18  $default[] = "visible_hostname senac_proxy";
19
20  $default[] = "acl manager proto cache_object";
21  $default[] = "acl localhost src 127.0.0.1/32 ::1";
22  $default[] = "acl to_localhost dst 127.0.0.0/8 0.0.0.0/32 ::1";
23
24  $default[] = "acl localnet src 10.10.0.0/16";
25
26  $default[] = "acl SSL_ports port 443";
27  $default[] = "acl Safe_ports port 80      # http";
28  $default[] = "acl Safe_ports port 21      # ftp";
29  $default[] = "acl Safe_ports port 443     # https";
30  $default[] = "acl Safe_ports port 70      # gopher";
31  $default[] = "acl Safe_ports port 210     # wais";
32  $default[] = "acl Safe_ports port 1025-65535 # unregistered ports";
33  $default[] = "acl Safe_ports port 280     # http-mgmt";
34  $default[] = "acl Safe_ports port 488     # gss-http";
35  $default[] = "acl Safe_ports port 591     # filemaker";
36  $default[] = "acl Safe_ports port 777     # multiling http";
37  $default[] = "acl CONNECT method CONNECT";
38
39  $default[] = "http_access allow manager localhost";
40  $default[] = "http_access deny manager";
41
42  $default[] = "http_access deny !Safe_ports";
43  $default[] = "http_access deny CONNECT !SSL_ports";
44

```

- A terceira parte contém a configuração das ACLs personalizadas. O funcionamento correto da aplicação depende dessa ordem.

```

46
47 /***** Cria ACLs e http_access do professor *****/
48
49 $acl[] = "##### ACLS PERSONALIZADAS #####";
50 $acl[] = "acl professor src \"\". $acl_pasta .\"professor\"";
51 $http_access[] = "http_access allow professor";
52
53
54 /***** Cria ACLs de sites_liberados *****/
55
56 $acl[] = "acl sites_liberados url_regex -i \"\". $acl_pasta .\"sites_liberados\"";
57 $ultimas_linhas[] = "http_access allow sites_liberados";
58
59 /***** Cria ACLs de sites_bloqueados *****/
60
61 $acl[] = "acl sites_bloqueados url_regex -i \"\". $acl_pasta .\"sites_bloqueados\"";
62 $ultimas_linhas[] = "http_access deny sites_bloqueados";
63
64 /***** Cria ACLs de palavras_bloqueadas *****/
65
66 $acl[] = "acl palavras_bloqueadas url_regex -i \"\". $acl_pasta .\"palavras_bloqueadas\"";
67 $ultimas_linhas[] = "http_access deny palavras_bloqueadas";
68
69 /*****
70
71 $ultimas_linhas[] = "http_access allow localnet";
72 $ultimas_linhas[] = "http_access allow localhost";
73 $ultimas_linhas[] = "http_access deny all";
74

```

- A quarta parte contém configurações relacionadas ao cache e o plugin **squidguard**. Modifique de acordo com a necessidade.

```

77 $ultimas_linhas[] = "##### CACHE #####";
78 $ultimas_linhas[] = "maximum_object_size_in_memory 1024 KB";
79 $ultimas_linhas[] = "maximum_object_size 100 MB";
80 $ultimas_linhas[] = "minimum_object_size 0 KB";
81 $ultimas_linhas[] = "half_closed_clients off";
82 $ultimas_linhas[] = "quick_abort_min -1";
83 $ultimas_linhas[] = "quick_abort_max -1";
84 $ultimas_linhas[] = "cache allow all";
85 $ultimas_linhas[] = "cache_swap_low 90";
86 $ultimas_linhas[] = "cache_swap_high 95";
87 $ultimas_linhas[] = "cache_replacement_policy heap LFUDA";
88 $ultimas_linhas[] = "memory_replacement_policy heap GDSF";
89 $ultimas_linhas[] = "cache_mem 6144 MB";
90 $ultimas_linhas[] = "cache_dir aufs /var/spool/squid 100000 32 256";
91 $ultimas_linhas[] = "coredump_dir /var/spool/squid";
92 $ultimas_linhas[] = "cache allow all";
93 $ultimas_linhas[] = "cache_log /var/log/squid/cache.log";
94
95 $ultimas_linhas[] = "##### REFRESH PATTERN #####";
96 $ultimas_linhas[] = "refresh_pattern ^ftp: 1440 20% 10080";
97 $ultimas_linhas[] = "refresh_pattern ^gopher: 1440 0% 1440";
98 $ultimas_linhas[] = "refresh_pattern -i (/cgi-bin/|\?) 0 0% 0";
99 $ultimas_linhas[] = "refresh_pattern . 0 20% 4320";
100
101 $ultimas_linhas[] = "##### SQUIDGUARD #####";
102 $ultimas_linhas[] = "url_rewrite_program /usr/local/bin/squidGuard -c /usr/local/squidGuard/";
103 $ultimas_linhas[] = "url_rewrite_children 20";
104
105 $ultimas_linhas[] = "max_filedescriptors 16384";
106

```

- A última parte do arquivo contém variáveis de configuração do DHCP. Essa configuração é necessária caso seja utilizada a funcionalidade da aplicação de gerar o arquivo **dhcpd.conf**.


```
108 /***** Variáveis para configurar o DHCP *****/
109
110 $dominio = "senacinformatica.br";
111 $dns1 = "10.10.0.1";
112 $dns2 = "10.10.255.254";
113 $default_lease_time = "600";
114 $max_lease_time = "7200";
115 $id = "10.10.0.0";
116 $netmask = "255.255.0.0";
117 $range = "10.10.100.1 10.10.200.254";
118 $option_router = "10.10.0.1";
119 $broadcast = "10.10.255.255";
```

10º - Ativando configuração de dhcp

Execute os comandos listados abaixo:

```
chown root.apache -R /etc/dhcp
```

```
chmod 774 -R /etc/dhcp
```

```
visudo
```

```
apache ALL=NOPASSWD:/etc/init.d/dhcpd
```

UTILIZAÇÃO

Abaixo listamos alguns requisitos básicos para utilização do Gsquid.

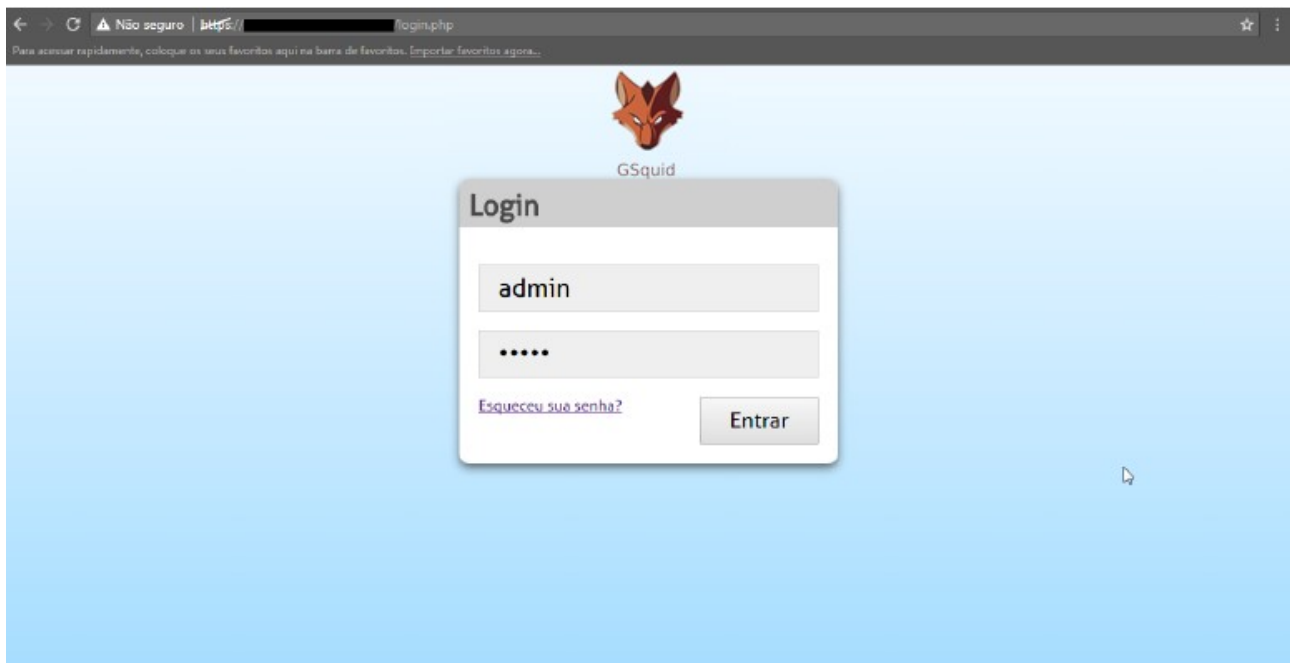
- **Navegadores:** Google Chrome, Firefox ou Microsoft Edge;
- **Javascript:** habilitado.

AUTENTICAÇÃO

Para acessar qualquer página da aplicação é necessário que o usuário esteja autenticado, caso contrário, o usuário será redirecionado à página de login.

As credencias dos usuários são criadas no menu “Usuários”. Como exemplo apresentamos credencias do usuário administrativo são:

- **Login:** admin
- **Senha:** System@77 (Esta senha é apenas um exemplo)

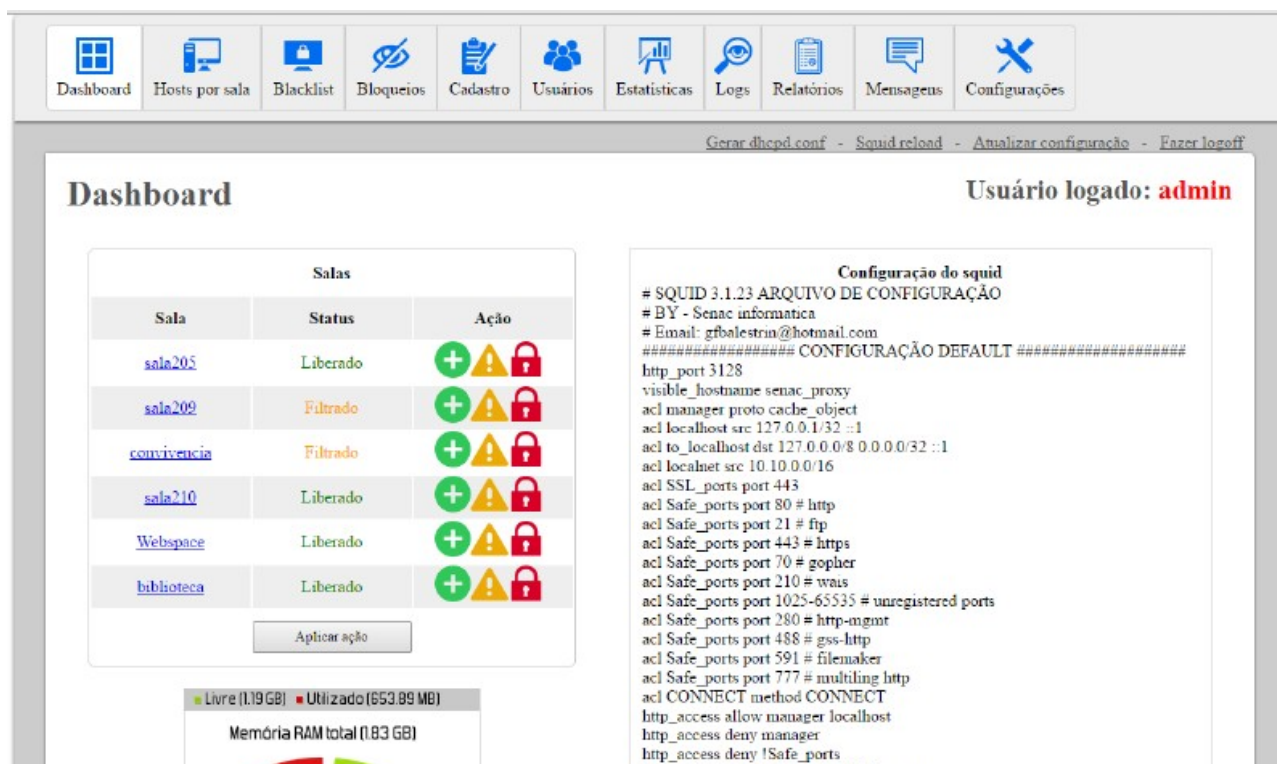


O usuário administrativo possui permissão para acessar diversos recursos da aplicação, como a configuração da aplicação e criação de usuários. Usuários sem privilégios administrativos possuem acesso limitado ao sistema.

DASHBOARD

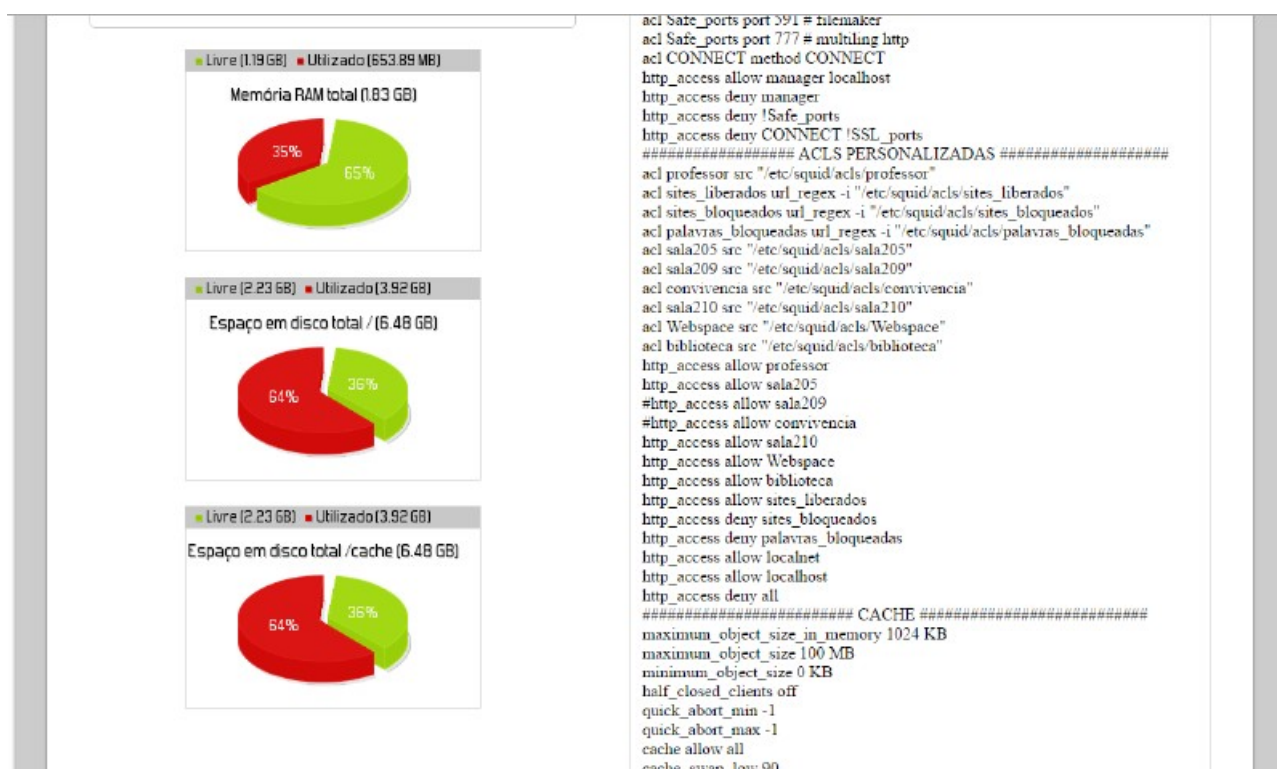
Após a autenticação correta na página de login o usuário será redirecionado à página principal, nomeada como **dashboard**. O **dashboard** administrativo possui três áreas:

- **Tabela de ações:** Permite a liberação, filtragem e bloqueio de internet por sala.
- **Gráficos do servidor:** Exibe informações sobre uso de disco e memória pelo servidor.
- **Configuração do squid:** Exibe a configuração atual do arquivo de configuração do squid.



Na figura acima temos o Dashboard administrativo. No lado esquerdo encontra-se a tabela de ações e no lado direito o início do arquivo de configuração do squid no estado atual.

No Dashboard administrativo. Logo abaixo da tabela de ações encontram-se gráficos sobre a utilização de recursos do servidor (Memória RAM, partição raiz e partição do cache). Como apresentado na figura abaixo.



A tabela de ações pode ser visualizada por usuários com perfil administrativo e por usuários com perfil de professor. No entanto, usuários com perfil professor só podem visualizar as salas de aula, e usuário com perfil administrativo conseguem visualizar salas da biblioteca, webspaces, convivência e TI.




Obs.: A ação só será aplicada após o clique no botão “Aplicar ação”

Na Tabela de Ações conforme mostra a figura abaixo, podemos encontrar na primeira coluna encontra-se o nome da sala cadastrada, cada sala contém computadores que podem ser visualizados clicando em cima do seu nome. A segunda coluna exibe o status de cada sala, que pode ser **Liberado**, **Filtrado** ou **Sem internet**. A terceira coluna exibe os botões de ação disponíveis para o usuário executar.

Salas		
Sala	Status	Ação
sala205	Liberado	  
sala209	Sem internet	  
convivencia	Filtrado	  
		<input type="button" value="Aplicar ação"/>

Obs.: Computadores com perfil de professor possuem acesso liberado e não serão afetados pelas ações de bloqueio. As ações são aplicadas somente a computadores com perfil aluno.

A figura a seguir explica as ações que podem ser adotadas no dashboard.

Ícone	Status	Descrição da ação
	Liberado	Libera acesso total à internet para determinada sala
	Filtrado	Determina que a sala acesse somente conteúdos que não são bloqueados pela aplicação. Os bloqueios são cadastrados na seção Bloqueios , que permite a configuração de sites bloqueados e palavras bloqueadas
	Sem internet	Nega o acesso à internet para a sala

Entre o menu superior e o conteúdo da página existem links com algumas ações importantes no sistema conforme figura abaixo que estão presentes em todas as páginas.

[Gerar dhcpd.conf](#) - [Squid reload](#) - [Atualizar configuração](#) - [Fazer logoff](#)

- **Gerar dhcpd.conf:** Esse link só será visto por usuários com privilégios administrativos. Essa ação gerará o arquivo de configuração do servidor DHCP, com endereço IP fixo para todos os computadores cadastrados no sistema.
- **Squid reload:** Esse link só será visto por usuários com privilégios administrativos. Essa ação executa a mesma ação do botão “Aplicar ação” localizado na página dashboard, que reinicializa a configuração do squid. Essa ação deve ser aplicada sempre que houver alguma alteração de configuração de computadores, salas, blacklists e bloqueios.
- **Atualizar configuração:** Esse link só será visto por usuários com privilégios administrativos. Essa opção fará com que a aplicação atualize toda a configuração do sistema. Essa ação é necessária quando o arquivo **config.php (arquivo de configuração do sistema)** for alterado.
- **Fazer logoff:** Esse link será visualizado por todos os usuários. Essa ação irá fechar a sessão do usuário, fazendo com que o usuário volte para a tela de autenticação.

HOSTS POR SALA

A página Hosts por sala exibe todos os computadores cadastrados no sistema, organizados pela sala na qual pertencem. Na coluna Ação é possível excluir um computador do sistema ou alterar sua configuração (Hostname, MAC, IP e Perfil).

Obs.: Clicando no endereço IP do computador é possível visualizar todos os acessos atuais do computador.

Dashboard

Hosts por sala

Blacklist

Bloqueios

Cadastro

Usuários

Estatísticas

Logs

Relatórios

Mensagens











Configurações

Gerar dhcpd.conf - Squid reload - Atualizar configuração - Fazer logout





Salas (14 computadores)

Usuário logado: admin

Computadores de sala205 (+)

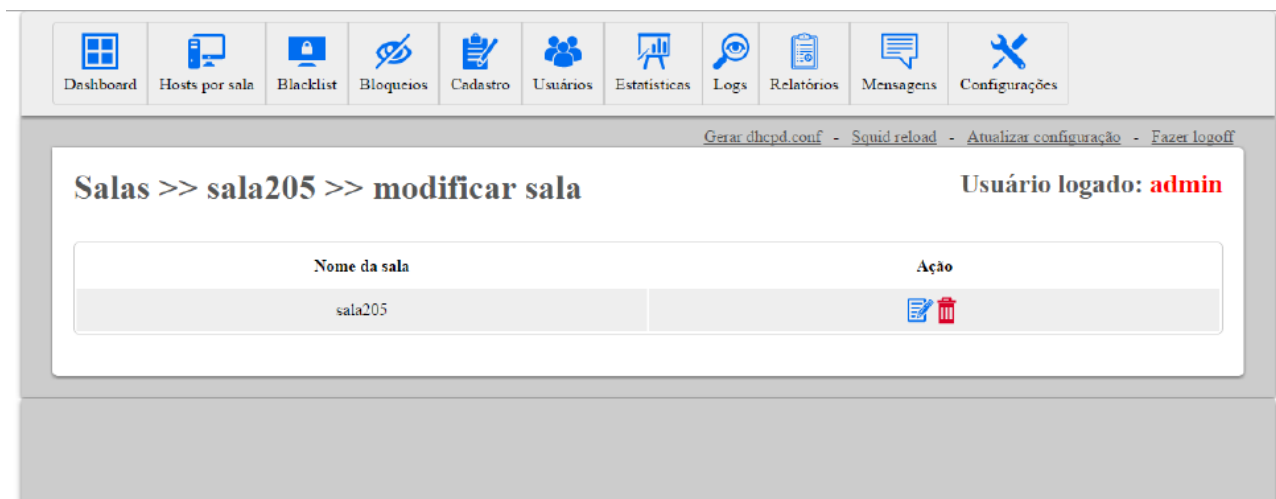
Hostname	MAC	IP	Perfil	Ação
LAB20507	64-1C-67-64-15-9A	10.10.104.235	professor	 
LAB20508	64-1C-67-64-1A-E9	10.10.104.240	aluno	 
LAB20509	64-1C-67-64-17-87	10.10.104.238	aluno	 
LAB20510	64-1C-67-62-72-45	10.10.104.242	aluno	 
LAB20511	64-1C-67-64-17-C7	10.10.104.241	aluno	 

Computadores de sala209 (+)

Hostname	MAC	IP	Perfil	Ação
LAB20901	64-1C-67-64-17-0F	10.10.3.137	professor	 
LAB20902	64-1C-67-62-5A-6B	10.10.3.138	aluno	 


Na página **Hosts por sala**, figura acima. O título principal da página exibe o número total de computadores cadastrados no sistema. Abaixo são exibidos todos os detalhes dos computadores cadastrados, organizados pelas salas na qual pertencem.

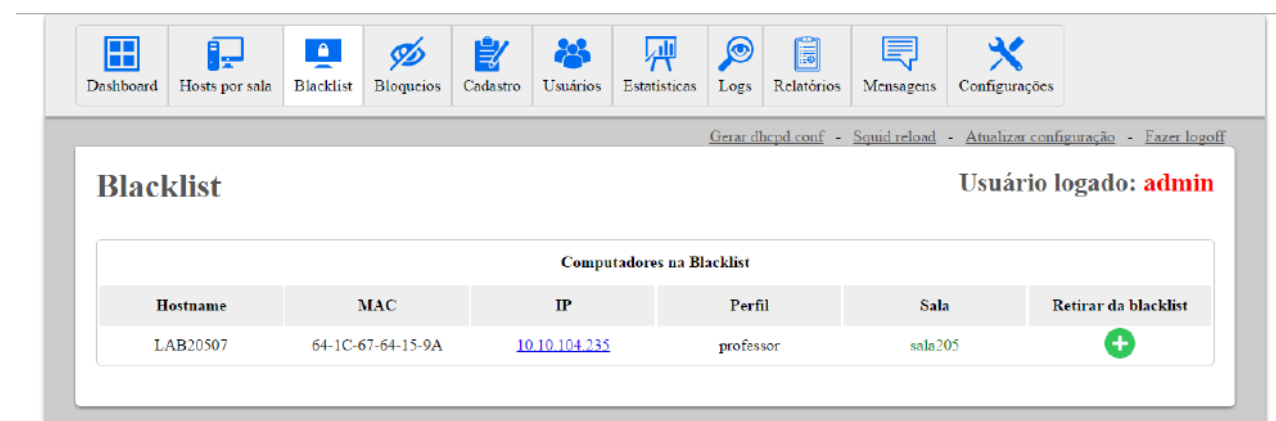
Obs.: Clicando no link **(+)** ao lado do nome da sala, é possível alterar seu nome ou excluí-la. Por questões de segurança, o sistema só irá permitir a exclusão da sala caso não exista computadores cadastrado.



Na figura acima percebemos a página de alteração do nome ou exclusão de sala.

BLACKLIST

A página Blacklist exibe computadores que estão em uma lista negra. Computadores na lista negra possuem seu acesso à internet bloqueado totalmente. Para retirar um computador da blacklist é necessário clicar no ícone  e reconfigurar o squid para aplicar a ação.



A página Blacklist exibida na figura acima apresenta todos os computadores inseridos na blacklist. Se o computador estiver cadastrado no sistema, será exibido informações referentes ao computador (Hostname, MAC, IP, perfil e Sala).

BLOQUEIOS

A página bloqueios tem como função controlar os bloqueios de sites, palavras e liberação de sites. A página possui três áreas:

- **Área para cadastro, alteração e exclusão de sites bloqueados:** sites que serão bloqueados pelo squid;
- **Área para cadastro, alteração e exclusão de palavras bloqueadas:** palavras-chave que serão bloqueadas pelo squid.
- **Área para cadastro, alteração e exclusão de sites liberados:** sites que não podem ser bloqueados, exceções em caso de bloqueio indesejado.

Obs.: Todos os bloqueios são realizados utilizando o elemento `url_regex` do proxy squid, que valida a URL através de expressão regular. Para mais informações acesse: <http://wiki.squid-cache.org/SquidFaq/SquidAcl>

Dashboard Hosts por sala Blacklist Bloqueios Cadastro Usuários Estatísticas Logs Relatórios Mensagens Configurações

Gerar dhcpd.conf - Squid reload - Atualizar configuração - Fazer logoff

Salas Usuário logado: **admin**

Site para bloqueio
Ex: .facebook.com
Cadastrar

Sites bloqueados

Site	Ação
youtube.com	[Edit] [Delete]
facebook.com	[Edit] [Delete]
.vimeo.com	[Edit] [Delete]

Palavras para bloqueio
Ex: sexo
Cadastrar

Palavras bloqueadas

Site	Ação
sexo	[Edit] [Delete]
tvonline	[Edit] [Delete]
gamesonline	[Edit] [Delete]

Sites Liberados
Ex: .senacrs.com.br
Cadastrar

Sites Liberados

Site	Ação
senacrs.com.br	[Edit] [Delete]

A figura acima traz a página **Bloqueios**. Essa página contém seções para gerenciar (inserção, alteração e exclusão) o bloqueio de sites, palavras e liberação de sites.

CADASTRO

A seção **Cadastro** é responsável pelo cadastro de **salas** e **computadores**.

O primeiro passo é o cadastro da sala, o sistema não permitirá o cadastro de um computador sem inseri-lo em uma sala. No cadastro da sala é possível habilitar por padrão o bloqueio de sites e palavras, ou desabilitar, fazendo com que a sala tenha acesso liberado à internet.

O cadastro de computadores deve ser realizado preenchendo obrigatoriamente todos os campos (Hostname, MAC, IP, Sala e Perfil), respeitando o formato exigido. O campo perfil permite somente duas opções:

- **Aluno:** computadores com perfil aluno terão acesso controlado pela tabela de ações na seção Dashboard.
- **Professor:** computadores com perfil professor terão sempre o acesso liberado, independente das ações executados na tabela de ações na seção Dashboard.

The screenshot shows the 'Cadastro' (Registration) page of a web application. The top navigation bar includes icons for Dashboard, Hosts por sala, Blacklist, Bloqueios, Cadastro, Usuários, Estatísticas, Logs, Relatórios, Mensagens, and Configurações. Below the navigation bar, there's a header with links: Gerar dhcpd.conf, Squid reload, Atualizar configuração, and Fazer logoff. The main content area is titled 'Cadastro' and shows 'Usuário logado: admin'. There are two main sections: 'Cadastro de computadores' and 'Cadastro de salas'. The 'Cadastro de computadores' section has fields for Hostname (Ex: LAB20201), MAC (Ex: FF-FF-FF-FF-FF-FF), IP (Ex: 10.0.0.1), Sala (a dropdown menu with '--- Selecione uma sala ---'), and Perfil (radio buttons for Aluno and Professor). The 'Cadastro de salas' section has a field for Sala (Ex: SALA202), a 'Bloqueios' section with radio buttons for Habilitar and Desabilitar, and a 'Cadastrar' button. Both sections have a 'Cadastrar' button at the bottom.

A figura acima apresenta a página **Cadastro**. Essa página possibilita o cadastro de salas de computadores.

USUÁRIOS

A página **Usuários** é responsável pelo cadastro, alteração e exclusão de usuários que terão acesso ao sistema. Existem dois níveis de permissão:

- **Usuários de nível 1:** Perfil Administrador. Possuem acesso total ao sistema e suas configurações.
- **Usuários de nível 2:** Perfil Docente. Possuem acesso somente à tabela de ações no Dashboard, à seção Mensagens e Configurações.

Obs: Ao realizar o cadastro de um usuário Docente ou a alteração de sua senha, o usuário será obrigado a alterar sua senha ao se autenticar. Essa medida de segurança garante que cada usuário defina obrigatoriamente sua própria senha.

Conforme demonstrado na figura abaixo, temos a página **Usuários**. Essa página possibilita o cadastro, alteração e exclusão de usuários.

Dashboard

Hosts por sala

Blacklist

Bloqueios

Cadastro

Usuários

Estatísticas

Logs

Relatórios

Mensagens

Configurações

Gerar dhcpd.conf - Squid reload - Atualizar configuração - Fazer logout

Usuários

Usuário logado: **admin**

Cadastro de usuário

Nome

Digite o nome

Senha

Digite a senha

Login

Digite o login





Email

Digite o email

Nível de permissão

☐ Administrador ☒ Docente

Cadastrar

Usuários						
ID	Nome	Login	Email	Nível	Senha	Ação
1	admin	admin	admin@senacrs.com.br	1	*****	 
8	professor	professor	professor@senacrs.com.br	2	*****	 

Obs: Por questões de segurança o sistema não irá permitir a exclusão de todos os administradores. É obrigatório a existência de ao menos um usuário com permissão administrativa.

ESTATÍSTICAS

A página **Estatísticas** exibe informações detalhadas de acessos e consumo de banda de hosts na rede.

No topo da página é exibido o número de linhas e tamanho dos arquivos de log atual e original do squid. O arquivo de log original consta de maneira acumulativa todos os acessos realizados, enquanto o arquivo de log atual exhibe somente os acessos que estão ocorrendo no turno atual.

A tabela abaixo contém todos os arquivos de acesso, separados por turno, dia, mês e ano. A coluna turno contém links que exibem informações de consumo de banda em determinado turno do dia e a coluna ação permite que os arquivos de acesso de determinado dia sejam excluídos.

Dashboard

Hosts por sala

Blacklist

Bloqueios

Cadastro

Usuários

Estatísticas

Logs

Relatórios

Mensagens

Configurações

Gerar dhcpd.conf - Squid reload - Atualizar configuração - Fazer logoff

Estatísticas

Usuário logado: admin


Log atual: 1553 linhas (292K)
Log original: 164207 linhas (28M)

Ano	Mês	Dia	Turno	Ação
2016	Abril	16	madrugada	
			manha	
			noite	
		17	tarde	
			madrugada	
			manha	
		18	noite	
			tarde	







Gerar estatísticas atuais

A página **Estatísticas** exhibe todos os arquivos de acesso, segmentados por turnos dos dias.

O sistema gerará automaticamente os arquivos de acesso no final de cada turno, porém os acessos que estão ocorrendo no atual momento podem ser visualizados através do botão “**Gerar estatísticas atuais**”. Essa ação pode ser executada manualmente diversas vezes, fazendo com que se tenha um monitoramento atual de consumo de banda.

		18	madrugada manha tarde	
Gerar estatísticas atuais				

Estatísticas Atuais

Consumo de banda por host					Consumo de banda por sala	
Endereço IP	Banda	Sala	Acessos	Ação	Sala	Banda
10.10.104.235	54.89 MB	sala205	Ver detalhes		sala205	94.36 MB
10.10.104.240	34.28 MB	sala205	Ver detalhes		sala209	2.87 MB
10.10.104.238	5.19 MB	sala205	Ver detalhes		convivencia	384.46 KB
10.10.100.129	3.68 MB	Não cadastrado	Ver detalhes		sala210	0 Bytes
10.10.3.137	2.87 MB	sala209	Ver detalhes		Webpace	0 Bytes
10.10.200.1	384.46 KB	convivencia	Ver detalhes		biblioteca	0 Bytes
Total: 101.28 MB						

Na página Estatísticas podemos mostrar o resultado da execução da ação “Gerar estatísticas atuais”. As estatísticas atuais são exibidas em duas tabelas, de “**consumo de banda por host**” e “**consumo de banda por sala**”.

A tabela de “**consumo de banda por sala**” soma o consumo de banda dos hosts que se encontram na mesma sala e exibe o consumo de banda total por cada sala.



Consumo de banda por sala	
Sala	Banda
sala205	36.1 MB
sala209	2.32 MB
convivencia	0 Bytes



Obs: O sistema só somará a banda de um host cadastrado no sistema. É possível que um host não cadastrado esteja em uma sala, por exemplo, uma máquina virtual.

A tabela de “**consumo de banda por host**” exibe de maneira decrescente os hosts que consumiram mais banda através do proxy. Se o endereço IP do host for cadastrado no sistema, seu endereço IP aparecerá como um link que irá o exibir informações sobre esse computador (Hostname, MAC, perfil) e a sala em que se encontra.

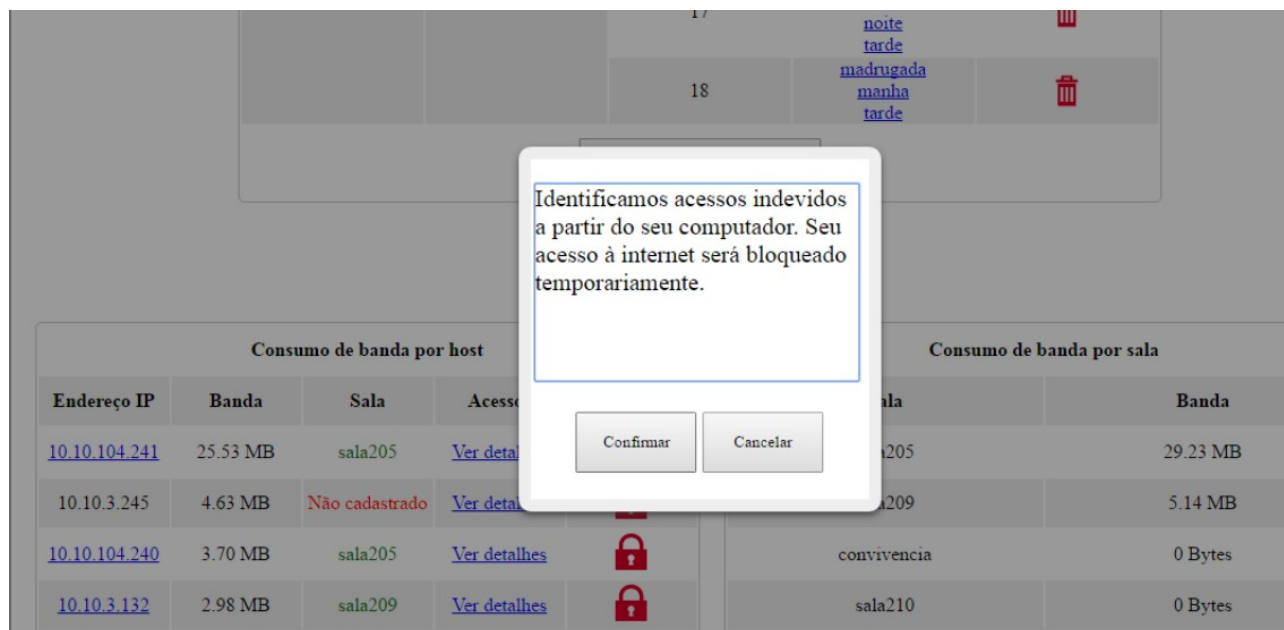
Consumo de banda por host				
Endereço IP	Banda	Sala	Acessos	Ação
10.10.104.235	26.55 MB	sala205	Ver detalhes	
10.10.104.240	9.55 MB	sala205	Ver detalhes	
10.10.100.137	7.32 MB	Não cadastrado	Ver detalhes	
10.10.3.137	2.30 MB	sala209	Ver detalhes	
10.10.100.129	105.19 KB	Não cadastrado	Ver detalhes	
10.10.3.129	15.50 KB	sala209	Ver detalhes	
Total: 45.84 MB				

Obs.: Caso o host não esteja cadastrado no sistema, a coluna sala irá exibir a informação “Não cadastrado”. Um host não cadastrado pode ser uma máquina virtual, ou também um host desconhecido inserido na rede.

A coluna **Ação** permite a inserção ou exclusão de determinado host na blacklist. O ícone  é exibido quando o host está inserido na blacklist, enquanto o ícone  é exibido quando o host não consta na blacklist. Abaixo a descrição das ações que podem ser executadas na página Estatísticas.

Ícone	Descrição da ação
	Retira o host da blacklist
	Inserir o host na blacklist

Ao inserir um host na blacklist, é necessário inserir uma mensagem personalizada. Essa mensagem será utilizada para avisar o usuário do host sobre o motivo do seu acesso à internet ter sido interrompido.

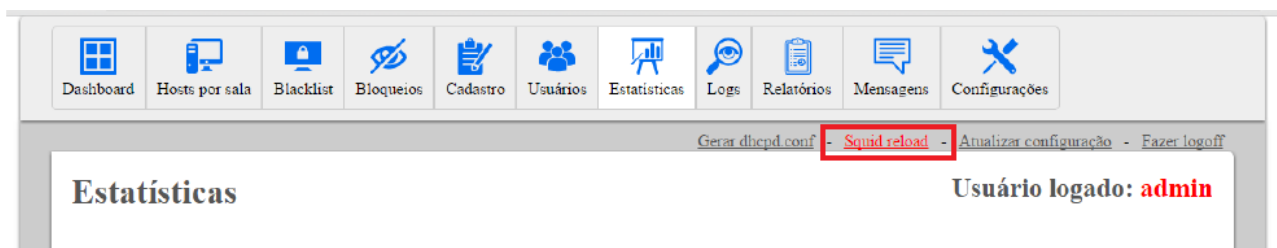


A figura acima demonstra um exemplo de mensagem que será visualizada pelo usuário do host que será inserido na blacklist. Logo em seguida será exibida a confirmação da inserção do host com endereço IP 10.10.104.241 na blacklist, conforme a figura abaixo.



Obs.: Ao confirmar a ação, será necessário reiniciar a configuração do squid, clicando em "Squid reload".

A reinicialização da configuração do squid, através do link **Squid reload**, confirme figura abaixo.



Após esse procedimento o host inserido na blacklist terá seu acesso à internet totalmente bloqueado, e a cada tentativa de acesso ele será redirecionado à uma página personalizada contendo a mensagem inserido anteriormente.



A figura acima demonstra a resposta a tentativa de acesso à internet a partir do host inserido na blacklist.

A coluna **Acessos** possibilita a visualização em detalhes de todos os acessos realizados por determinado host. É possível visualizar o site acessado, horário em que foi acessado, tamanho de download e código de status.

		18	tarde madrugada manha tarde	
<input type="button" value="Gerar estatísticas atuais"/>				

Estatísticas Atuais

Consumo de banda por host				
Endereço IP	Banda	Sala	Acessos	Ação
10.10.104.241	25.54 MB	sala205	Ver detalhes	
10.10.3.245	4.97 MB	Não cadastrado	Ver detalhes	
10.10.104.240	4.11 MB	sala205	Ver detalhes	
10.10.3.132	3.10 MB	sala209	Ver detalhes	
10.10.3.129	2.95 MB	sala209	Ver detalhes	
Total: 40.65 MB				

Consumo de banda por sala	
Sala	Banda
sala205	29.64 MB
sala209	6.05 MB
convivencia	0 Bytes
sala210	0 Bytes
Webspace	0 Bytes
biblioteca	0 Bytes

A página **Estatísticas**. Exibindo detalhes de acesso do host com endereço IP 10.10.104.241.

É possível organizar a lista de acessos por data (clcando no link Data) ou por tamanho da requisição (clcando no link Bytes).

Gerar dhcpd.conf - Squid.reload - Atualizar configuração - Fazer logoff

Estatísticas >> detalhes

Usuário logado: admin

O endereço 10.10.104.241 realizou 802 acessos

1

Acessos de 10.10.104.241

Site	Data	Bytes	Flag
http://www.ncsi.com/ncsi.txt	27/05/2018 15:18:01	389 Bytes	TCP_DENIED:302
http://www.terra.com.br/	27/05/2018 15:17:54	394 Bytes	TCP_DENIED:302
www.google.com:443	27/05/2018 15:17:54	395 Bytes	TCP_DENIED:307
safebrowsing-cache.google.com:443	27/05/2018 15:12:36	2.33 MB	TCP_MISS:200
safebrowsing.google.com:443	27/05/2018 15:12:32	8.39 KB	TCP_MISS:200
ads.rubiconproject.com:443	27/05/2016 15:11:39	11.87 KB	TCP_MISS:200
clients1.google.com:443	27/05/2018 15:11:11	959 Bytes	TCP_MISS:200
tpc.google syndication.com:443	27/05/2018 15:10:48	138.6 KB	TCP_MISS:200
securepubads.g.doubleclick.net:443	27/05/2018 15:10:46	80.63 KB	TCP_MISS:200
stats.g.doubleclick.net:443	27/05/2018 15:10:46	5.64 KB	TCP_MISS:200
s0.2mdn.net:443	27/05/2018 15:10:45	39 KB	TCP_MISS:200
www.google-analytics.com:443	27/05/2018 15:10:38	5.22 KB	TCP_MISS:200
www.google.com:443	27/05/2018 15:10:05	4.82 KB	TCP_MISS:200
s.glbimg.com:443	27/05/2018 15:09:43	4.39 KB	TCP_MISS:200
clients1.google.com:443	27/05/2018 15:09:12	32.02 KB	TCP_MISS:200


Na figura acima podemos perceber detalhes de acessos realizados pelo host com endereço IP 10.10.104.241.

Obs.: A coluna Flag exibe o código de status, que representa a ação tomada pelo squid em determinado acesso. Exemplos de Flags:

- TCP_DENIED: acesso negado;
- TCP_MISS: acesso permitido e realizado através da rede;
- TCP_HIT: acesso permitido e realizado através do cache local.

Para informações mais detalhadas acesse:

<http://wiki.squid-cache.org/SquidFaq/SquidLogs>

Da mesma que na página Estatísticas é possível inserir o host na blacklist, quando clicamos no ícone  localizado no canto superior direito da página. O processo de inserção é o mesmo aplicado no exemplo anterior.

Dashboard

Hosts por sala

Blacklist

Bloqueios

Cadastro

Usuários

Estatísticas

Logs

Relatórios

Mensagens


Configurações

Gerar dhcpd.conf - Squid reload - Atualizar configuração - Fazer logout

Estatísticas >> detalhes

Usuário logado: admin

O endereço 10.10.104.241 realizou 802 acessos

 bloquear

Acessos de 10.10.104.241