By Sean
Published: 2008-07-29 15:11

How To Control Or Block Instant Messengers With SafeSquid Proxy Server

In this tutorial I will explain how you can control or completely block access to a few instant messengers with SafeSquid, like Google Talk, Google chat within Gmail, MSNMessenger, Yahoo Messenger and Skype. Once you are familiar with the method of blocking these messengers, you should be able to block other messengers. Please note that thesemethods will only be effective, if you block all direct access to the router and firewall, except required ports like 25 & 110, so that users are able to access the net onlythrough the proxy server. When all higher ports are blocked, most messenger try to communicate on port 80 and 443, which will have to go through the proxy, and thus allow you tocontrol them. Most messengers also allow you to define proxy settings and username / password for authenticating Proxies.

Google Talk Client:

Once you have defined the proxy settings in a messenger, you can trace the requests made by the messenger, in the SafeSquid Extended Logs. For example, ifyou specify the proxy settings in Google Talk client (Settings => connection) and suppose your system's IP address is 192.168.0.8, to trace the requests made by this system inthe extended.log, use the following command:

```
tail -f /opt/safesquid/safesquid/logs/extended/extended.log | grep 192.168.0.8
```

Now, when you sign into the Google Talk client, you should see entries similar to this in the log:

```
"1215860434.313-2662-192.168.0.175-8080" 787 192.168.0.8 "anonymous@192.168.0.8" "2662" [12/Jul/2008:07:00:35] "CONNECT
connect://www.google.com:443/" 0 0 "-" "Google Talk" - "- -" "-" "192.168.0.175:8080"
```

The various fields in the above entry, are as follows:

```
"UNIQUE_RECORDID" ELAPSED_TIME_IN_MSEC CLIENT_IP "USER_NAME" "CLIENT_CONNECTION_ID" [DATE_TIME_OF_REQUEST] "METHOD URL"
HTTP_STATUS_CODE BYTES_TRANSFERRED "REFERRER_URL" "USER_AGENT" MIME_TYPE "FILTER_NAME" "FILTERING_REASON"
"COMMA_SEPARATED_LIST_OF_PROFILES_APPLIED""INTERFACE_IP:INTERFACE_PORT"
```

The unique field in this request is *USER_AGENT*, since it identifies the application (Google Talk Client) that is making the request - *GoogleTalk*. This will be reflected in the request headers of the requests from the GTalk client. You can now create a profile to identify the requests made by the GTalk client,and use that profile in the *URL filter* section, to block unwanted requests.

To create a profile, go to *Config* => *Profiles*, click on *Add* under the *Profile*subsection, and create the following profile:

Option	**Value**
Enabled	true
Comment	Apply profile 'Block-GTalk' to the specified profiles
Profiles	Accounts,Finance
Request header pattern	User-Agent: Google Talk
Hour range	9,18
Time match mode	absolutetime
Added profiles	Block-GTalk

Note the *Request header pattern* field and it's value - *User-Agent: Google Talk*. The entry *User-Agent:Google Talk* is a regular expression that will identify requests made by GTalk client.

The above rule will apply profile *Block-GTalk* to requests made by users from *Accounts* and *Finance*group using the GTalk client between 9 hrs & 18 hrs. If you would like to apply the profile *Block-GTalk* to everyone, just leave the *Profiles*field blank. You can also skip the *Hour range*, if you would not want to select any time range.

Next, go to *Config* => *URL filter* section, click on *Add* under *Deny*subsection, and create the following rule (presuming *Policy* is *Allow*):

Option	**Value**
Enabled	true
Comment	Block 'Block-GTalk' profile
Profiles	Block-GTalk

This rule will block requests carrying *Block-GTalk* profile.

Google chat within gmail:

Google chat within Gmail can simply be blocked by blocking the URL - *chatenabled.mail.google.com*. This will allow the users toaccess gmail normally, but block chat within gmail. Just create the following profile under *Profiles* section:

Option	Value
Enabled	true
Comment	Apply profile 'Chat-Enabled-Gmail' to the specified profiles
Profiles	Accounts,Finance
Host	chatenabled.mail.google.com
Hour range	9,18
Time match mode	absolutetime
Added profiles	Chat-Enabled-Gmail

Then block the profile *Chat-Enabled-Gmail* under *URL filter* section:

Option	Value
Enabled	true
Comment	Block 'Chat-Enabled-Gmail' profile
Profiles	Chat-Enabled-Gmail

MSN Messenger:

When you trace requests made by the MSN Messenger client, you should get an entry similar to this:

```
"1216019587.598-3249-192.168.0.175-8080" 683 192.168.0.8 "anonymous@192.168.0.8" "3249" [14/Jul/2008:03:13:08] "POST
http://gateway.messenger.hotmail.com:80/gateway/gateway.dll?Action=open&Server=NS&IP=messenger.hotmail.com" 200 26 "-"
"Mozilla/4.0 (compatible; MSIE7.0; Windows NT 5.1; InfoPath.2; FDM; .NET CLR 2.0.50727; MSN Messenger 7.0.0816)"
application/x-msn-messenger "- -" "-" "192.168.0.175:8080"
```

As you can see, there are three unique fields in the above request, namely:

- **URL** - http://gateway.messenger.hotmail.com
- **User Agent** - "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; InfoPath.2; FDM; .NET CLR 2.0.50727; **MSN Messenger** 7.0.0816)", and
- **Mime Type** - application/x-msn-messenger

So you can create a profile for MSN Messenger, based on either of the three unique fields:

Based on URL:

Option	Value
Enabled	true
Comment	Apply profile 'Block-MSN-MSG' to the specified profiles
Profiles	Accounts,Finance
Host	gateway.messenger.hotmail.com
Hour range	9,18
Time match mode	absolutetime
Added profiles	Block-MSN-MSG

Based on User Agent:

Option	Value
Enabled	true
Comment	Apply profile 'Block-MSN-MSG' to the specified profiles
Profiles	Accounts,Finance
Request header pattern	User-Agent: .*MSN Messenger.*
Hour range	9,18
Time match mode	absolutetime
Added profiles	Block-MSN-MSG

Based on Mime type:

Option	Value
Enabled	true
Comment	Apply profile 'Block-MSN-MSG' to the specified profiles
Profiles	Accounts,Finance
Mime type	^application/x-msn-messenger
Hour range	9,18
Time match mode	absolutetime

Added profiles	Block-MSN-MSG

The profiles created using URL and User Agent, can then be blocked under *URL filter* section, similar to blocking GTalk.
The profile created using Mime type, can be blocked using the *Mime Filter* section.

Yahoo Messenger:

Tracing a request made from Yahoo Messenger should give an entry similar to this:

```
"1215865434.285-2726-192.168.0.175-8080" 1564 192.168.0.15 "anonymous@192.168.0.15" "2726" [12/Jul/2008:08:23:55] "POST
http://shttp.msg.yahoo.com:80/notify/" 200 116 "SHRI" "Mozilla/4.01 [en] (Win95; I)" text/plain "- -" "-""192.168.0.175:8080"
```

You do not have much choice here, since the only unique field in this request is the URL - shttp.msg.yahoo.com
So you can create a profile based on this URL and use it under the URL filter to block Yahoo Messenger:

Option	**Value**
Enabled	true
Comment	Apply profile 'Block-Yahoo-MSG' to the specified profiles
Profiles	Accounts,Finance
Host	shttp.msg.yahoo.com
Hour range	9,18
Time match mode	absolutetime
Added profiles	Block-Yahoo-MSG

Please note that this rule will only control Yahoo Chat, File Sharing and File Transfer. Other services like Webcam and Voice Chat require a direct access, and can not gothrough a proxy. The protocol, Servers and Ports used by these services are as follows:

Service	**Protocol**	**Server**	**Ports**
Yahoo Webcam	TCP	webcam.yahoo.com	5100
Voice Chat	UDP or TCP	v1.vc.scd.yahoo.com	
		v2.vc.scd.yahoo.com	
		v3.vc.scd.yahoo.com	
		v4.vc.scd.yahoo.com	
		v5.vc.scd.yahoo.com	

v6.vc.scd.yahoo.com
v7.vc.scd.yahoo.com
v8.vc.scd.yahoo.com
v9.vc.scd.yahoo.com
v10.vc.scd.yahoo.com
v11.vc.scd.yahoo.com
v13.vc.sc5.yahoo.com
vc1.vip.scd.yahoo.com 5000-5010

Skype:

Skype is the most difficult to control, since it does not have any unique field. It does not even have a fixed URL that it tries to connect, but has a listof Super Nodes that it tries to connect, based on their IPs. Tracing the extended log for Skype, gives entries similar to this:

```
"1216022851.657-3-192.168.0.175-8080" 362 192.168.0.8 "anonymous@192.168.0.8" "3" [14/Jul/2008:04:07:32] "CONNECT
connect://99.245.19.125:443/" 0 0 "-" "-" - "- -" "-" "192.168.0.175:8080"
"1216022849.608-2-192.168.0.175-8080" 7937 192.168.0.8 "anonymous@192.168.0.8" "2" [14/Jul/2008:04:07:37] "CONNECT
connect://98.221.64.42:443/" 0 0 "-" "-" - "- -" "-" "192.168.0.175:8080"
"1216022950.516-10-192.168.0.175-8080" 338157 192.168.0.8 "anonymous@192.168.0.8" "10" [14/Jul/2008:04:14:48] "CONNECT
connect://89.78.13.89:443/" 0 0 "-" "-" - "- -" "-" "192.168.0.175:8080"
"1216022947.512-8-192.168.0.175-8080" 341161 192.168.0.8 "anonymous@192.168.0.8" "8" [14/Jul/2008:04:14:48] "CONNECT
connect://89.32.208.250:443/" 0 0 "-" "-" - "- -" "-" "192.168.0.175:8080"
"1216022940.019-7-192.168.0.175-8080" 348655 192.168.0.8 "anonymous@192.168.0.8" "7" [14/Jul/2008:04:14:48] "CONNECT
connect://89.102.163.62:443/" 0 0 "-" "-" - "- -" "-" "192.168.0.175:8080"
"1216022933.502-5-192.168.0.175-8080" 355172 192.168.0.8 "anonymous@192.168.0.8" "5" [14/Jul/2008:04:14:48] "CONNECT
connect://89.35.204.65:443/" 0 0 "-" "-" - "- -" "-" "192.168.0.175:8080"
```

Note that the requests are CONNECT requests, or HTTPS requests. Also note that the IP addresses keep changing. These are the IP addresses of the Super Nodes.

So the only unique thing about these requests are that:
- The requests are connect, or https requests
- The requests are IP based

Based on these inference, we can create the following profile, and use it under *URL filter* section, to block Skype:

Option	Value
Enabled	true
Comment	Apply profile 'Block-Skype' to the specified profiles
Profiles	Accounts,Finance
Protocol	^connect$
Host	^[0-9]+.[0-9]+.[0-9]+.[0-9]+
Hour range	9,18
Time match mode	absolutetime
Added profiles	Block-Skype

The above rule will block all IP based connect requests. This very effectively blocks Skype.
Now if you trace the requests from Skype in the extended log, you should see entries like these:

```
"1216024002.264-514-192.168.0.175-8080" 2 192.168.0.8 "anonymous@192.168.0.8" "514" [14/Jul/2008:04:26:42] "CONNECT
connect://79.132.75.51:443/" 404 7871 "-" "-" text/html "url-filter -" "Block-Skype" "192.168.0.175:8080"
"1216024019.464-515-192.168.0.175-8080" 2 192.168.0.8 "anonymous@192.168.0.8" "515" [14/Jul/2008:04:26:59] "CONNECT
connect://66.229.116.97:443/" 404 7872 "-" "-" text/html "url-filter -" "Block-Skype" "192.168.0.175:8080"
"1216024019.468-516-192.168.0.175-8080" 2 192.168.0.8 "anonymous@192.168.0.8" "516" [14/Jul/2008:04:26:59] "CONNECT
connect://66.67.85.138:443/" 404 7871 "-" "-" text/html "url-filter -" "Block-Skype" "192.168.0.175:8080"
"1216024040.890-517-192.168.0.175-8080" 2 192.168.0.8 "anonymous@192.168.0.8" "517" [14/Jul/2008:04:27:20] "CONNECT
connect://98.212.7.209:443/" 404 7871 "-" "-" text/html "url-filter -" "Block-Skype" "192.168.0.175:8080"
```

Note the Applied profile - *Block-Skype* and Filter name - *url-filter*

The only rare problem that this rule might cause, is that it might block access to some valid IP based HTTPS site. To overcome this problem, just create another profile belowthis rule, like this:

Option	Value
Enabled	true
Comment	Remove profile 'Block-Skype' applied to the specified hosts
Protocol	^connect$

Host 82.103.135.130
Time match mode absolutetime
Removed profiles Block-Skype

The above rule will remove the profile (`Removed profiles`) Block-Skype when a connect request is made to IPs specified in the `Host`field. You can specify multiple IP addresses separated with pipe.

Also see:

- **Deploying A Content Filtering Proxy Server To Distribute Controlled Internet Access With SafeSquid**
- **Set Up Gateway Level Virus Security With ClamAV And SafeSquid Proxy**
- **How To Set Up Internet Access Control And Internet Filtering With SafeSquid Proxy Server**
- **How To Control Access To Unwanted Websites Using URL Blacklist With SafeSquid Proxy Server**
- **How To Configure Granular Bandwidth Management Rules In SafeSquid Proxy Server**
- **How To Control Download Of Files And Mime Types In SafeSquid Proxy Server**
- **How To Block Ads And Banners In SafeSquid Proxy Server**
- **How To Block Cookies From Unwanted Websites With SafeSquid Proxy Server**
- **Enhance Security By Removing ActiveX Control Codes From Web Pages With SafeSquid Proxy Server**