

Gameserver Protector

Description / Purpose

GsProtector is the tool that helps to protect your game server and also offers additional admin features, Features:

- Protection against ddos attacks
- Protection against query flood attacks (e.g. getstatus flood)
- If your server is being attacked you will still be able to join and play
- Protection against rcon flooding
- Protection against remote crashing
- Protection against attacks with spoofed IP's
- Autoban System for Attackers
- Anti Lag
- IP Banning
- IP Range Banning
- Immunelist
- Rconlocker: Prevents changing of rcon password via console
- Whitelists for Queries, Rcon, Joining
- Shield Mode
- Detailed Information about Packets and Traffic
- Easy to use Sub-Admin System, Sub Admins get their own rcon password so they can use any other rcon tool e.g. scapp-host, ingame menu or ingame console - you define which commands they allowed to use
- Fully configurable via config file or rcon, features can be toggled on/off
- High Performant, as effectively as a firewall but especially tailored for game servers
- Works independently from other patches or tools
- Very easy to install, only FTP access is required

Installation

Extract the zip archiv and place the files in your root game server folder (there where the game server executable is) and restart your game server.

(**Important:** Please change the passwords in the GsProtector.ini file: **rconpw** and **loginpw** to strong passwords.)

You should then when you start your server see a GsProtector_logfile.txt generated in your server folder. You can also test with a rcon gpstatus if all is setup properly.

Deinstallation

Remove (all) the files (that are associated with GsProtector) from your root game server folder and restart your game server.

Anti Flooding / Anti Lag and Auto ban Flooders

Banning

Sub Admin System

Available Sub Admin Commands:

gpinfo
gpstatus
echo

status
kick <Name>
say <String>
clientkick <ClientSlotNumber>
map <String>
gametype <GameTypeNumber>
exec <String>
set <String>
cmd <String>
quit
gpanip <IP>
gpunbanip <IP>
restart
dumpuser <String>

How Sub Admin Works:

To enable and allow Sub Admins you set the parameter AllowSubAdmins to 1 in the GsProtector.ini file.

Further you have to set the servers real rconpassword in this parameter: Rconpassword

You set the commands your Sub Admins with the parameter: SubAdminsAllowedCommands. Possible values are from 0 to 16384, check below on how to set which commands are allowed.

Finally you set the Sub Admin Password in this parameter: SubAdminPw.

Your Sub Admins can use this password as if it is the rconpassword of the server, so they can use it with any rcon tool or from console, but only allowed commands will work.

Important, Please Note:

>>>>>>> The Subadmin Password must be longer or equal in length than the Server Rcon Password <<<<<<<<<<

Setting Rights for Sub Admin:

The following commands are associated with a value:

Command	off-value	on-value
status	0	1
kick	0	2
say	0	4
clientkick	0	8
map	0	16
gametype	0	32
exec	0	64
set	0	128
gpanip	0	256
gpunbanip	0	512
cmd	0	1024
quit	0	2048
restart	0	4096
dumpuser	0	8192

Now you have to do some math, you have to add the values of the commands you want to allow and set the param SubAdminsAllowedCommands accordingly.

Example:

you want to allow status, clientkick, say, gpanip and dumpuser then your table looks like this: (for all commands we dont want to allow we take the off-value 0, else the on-value from above list)

status	1
kick	0
say	4
clientkick	8
map	0
gametype	0
exec	0
set	0
gpanip	256
gpunbanip	0
cmd	0
quit	0
restart	0
dumpuser	8192

The sum is: 8461

You now set the parameter SubAdminsAllowedCommands to 8461. Thats it.

Additional Sub-Admin Passwords:

You can define additional sub-admin passwords in the GsProtector_SubAdmins.txt file.

The syntax is: "<password>" <Rights>

for example: "ThisIsATestPassword" 5

Important are the Quotes around the password, and please remember that sub-admin password have to be longer (or equal) in length than the server's rcon password.

Please note: gpinfo, gpstatus and echo will always work hence no value. (echo is a command which is used by many rcon tools for testing if the rcon password is correct)

Firewall bans

GsProtector offers the ability to issue IP bans directly in the windows firewall.

To make use of this option the gameserver has to be started with sufficient rights, usually as administrator, and the settings have to be set accordingly which are:

pathToNetsh: the path to netsh.exe, usually "c:\Windows\System32\netsh.exe"

appPort: the listening port of your gameserver e.g. 12203. This is used as identifier in the firewall, aswell as blocking the IP only for this specific port (this applies to winserver 2008/win7 only, on win2003/win2000/xp all ports will be banned for that IP)

FirewallBans: set here whether to allow firewall bans or not

Please note: If firewall bans aren't allowed and Banning is set to 2 no bans will be issued

Caution on win2003/2000/xp server, if u test-ban yourself make sure you can access the firewall somehow.

The Config Files

GsProtector is controlled via 2 config files: GsProtector.ini and GsProtector_Host.ini

The GsProtector_Host.ini has settings for the Gameserver Hoster:

Code: [\[Select\]](#)

```
[common]
FirewallBans=0
OperatingSystem=0
GameType=0
pathToNetsh="c:\Windows\System32\netsh.exe"
appPort="12203"
```

FirewallBans: wheter to allow (1) or disallow (0) bans in the firewall of the windows server.

OperatingSystem: 0= WinServer2008/ Win7/Vista, 1= WinServer 2000/2003/XP

GameType: The type of the Gameserver, e.g. 0=Mohaa, 1= Spearhead/Breakthrough

pathToNetsh: The full path to the netsh.exe command line tool (required for firewall control)

appPort: The listening Port of the gameserver. Also used as identifier for bans in the firewall

The GsProtector.ini has these settings:

Code: [\[Select\]](#)

```
[common]
Banning=1
AntiFlood=1
AutoBanFloods=1
MaxQueriesPerSec=50
MaxRconPerSec=10
MaxConnectPerSec=10
PrintInfo=1
AutoUnBan=3
AutoUnBanHours=24
WlQueries=0
WlRcon=0
WlJoin=0
ImmuneList=1
Logging=1
FloodValueMs=50
FloodPacketsThreshold=5
FloodPacketsIP=20
performChallenge=0
UpdateConfigOnRcon=1
MaxConnPerIP=5
LimitConnPerIP=0
IpRangeBans=1
AllowAddRangeBansViaRcon=1
RconLocker=1
rconpw="thepw"
gploginpw="thepw"
```

Banning: 0=off, 1= internal bans only, 2 = firewall bans only, 3 = internal and firewall bans

Shielding and Login

This is a mode meant mainly for war servers.

Players register with the server by doing a login. War admin handles out the gploginpw to the players, they do a "rcon <gploginpw> login" in their ingame console or via a rcon tool.

Now the war admin sets the Shield to 1 and the server is in shield-mode which means only those players previously logged in can join or play, getstatus queries to the server are limited and also only those player registered can issue rcon commands.

It is like a passworded server with the addition that it also cares about query and rcon requests.

Whitelists and Immunelists

GsProtector offers Whitelist for Join/Connected Players, Rcon and Queries and an Immunelist to immunisize IP's.

Immunelist: No checks will be done for network packets that come from IP that have been immunisized Rcon command to add IP to the Immunelist: ImmuneAdd <IP>

Rcon command to remove IP from the Immunelist: ImmuneRem <IP>

Whitelist: IP's on a Whitelist are exclusively allowed for the server if the specific whitelist is turned on.

Rcon command to add IP to a Whitelist: WlAdd <WlType> <IP> wlType: [0,1,2]

(0=queries, 1=rcon, 2= join)

Rcon command to remove IP from a Whitelist: WlAdd <WlType> <IP> wlType: [0,1,2]

(0=queries, 1=rcon, 2= join)

You need to specify to which Whitelist you want to add the IP with the WlType.

Example:

As Admin of your server you want to be the only one allowed to issue rcon commands in the server, then you add your IP to the Rcon Whitelist: rcon WlAdd 1 192.168.0.255

Where 1 specifies the type of the Whitelist = here Rcon and 192.168.0.255 is your actual IP.

Now you turn on the Whitelist for Rcon with: rcon WlRcon 1

Alternatively you can also do a login with the server (as described in Topic Shielding) which adds your IP automatically to all Whitelists and turn on the Whitelist for Rcon only.

Remote Crash Fixes

The GsProtector protects versus different remote crash attacks.

However it does not fix any vulnerabilities that are related to the gameserver engine itself like mohbuf fill attack.

Log files

These logfiles will be created:

GsProtector_logfile.txt

Contains info about the status of GsProtector

If Logging is set to 1 then Rcon, Player Connects will be written to log files.

If PrintInfo is set 1 information about the packets that have been sent to the gameserver in a timeinterval like how many queries, how many banned packets will be written to the log file.

example of the content:

Code: [\[Select\]](#)

```
=====Sun Apr 01 17:23:40 2012
    Config settings loaded, GS Protector working.
```

```
=====Sun Apr 01 17:23:40 2012
    Gameserver Protector Current Config Settings:
OperatingSystem= 0
appPort= 12203
loginpw= test
Banning= 1
AntiFlood= 1
AntiLag= 1
MaxQueriesPerSec= 50
MaxRconPerSec= 10
MaxConnectPerSec= 10
PrintInfo= 1
AutoUnBan= 3
AutoUnBanHours= 24
WlQueries= 0
WlRcon= 0
WlJoin= 0
ImmuneList= 1
```

```
Logging= 1
FloodPacketsMs= 50
FloodPacketsThreshold= 5
FloodPacketsIP= 10
performChallenge= 0
Shield= 0

=====Sun Apr 01 17:25:42 2012
Received Packets Info.
Timespan: 60001 ms
Packets: 16
Queries: 16
Banned Packets: 0
Connect Packets: 0
Rcon Packets: 0
```

GsProtector_PlayerConnectDetails.txt

Details of the player connecting to the gameserver will be written into this file.

GsProtector_log_attacking_IPs.txt

If an attac is detected the IP of the attacker is written to this file.

Rcon Commands

These are Rcon Commands you can use:

Code: [\[Select\]](#)

```
Banning          [0,1,2,3]    (0=off, 1=internal bans, 2=firewall bans, 3=
internal + firewall bans)
AntiFlood         [0,1]
AutoBanFloods     [0,1]
MaxQueriesPerSec  [10-9999]
MaxRconPerSec     [10-9999]
MaxConnectPerSec  [10-9999]
PrintInfo         [0,1]
AutoUnBan         [0,1]
AutoUnBanHours    [1-9999]
WlQueries         [0,1]
WlRcon            [0,1]
WlJoin           [0,1]
ImmuneList        [0,1]
Logging           [0,1]
FloodValueMs      [20-750]    (1000ms = 1000 milliseconds = 1 second)
FloodPacketsThreshold [3-50]
FloodPacketsIP    [3-50]
performChallenge  [0,1]
UpdateConfigOnRcon [0,1]
Gploginpw         <String>    (Passwords max. 30 chars long,
minimum length 3)
GpReset
GpStatus
GpDefault
GpInfo
```

```

MaxConnPerIP      [1-100]
LimitConnPerIP    [0,1]
IpRangeBans       [0,1]
ReloadBans
GpBanIP <IP>
GpUnbanIP <IP>
WlAdd <WlType> <IP>      wlType: [0,1,2] (0=queries, 1=rcon, 2= join)
WlRem <WlType> <IP>      wlType: [0,1,2] (0=queries, 1=rcon, 2= join)
ImmuneAdd <IP>
ImmuneRem <IP>
SubAdminPw                <String>
Rconpassword               <String>
SubAdminsAllowedCommands  [0-16384]

```

In brackets the possible values.

Please note:

1)GpBanIP and GpUnbanIP accept IP's in 3 different formats:

1.1) IP in format e.g. 224.0.0.1 ==> the Ban will be added/removed to the IP Banlist

1.2) IP in format e.g. 224.0.0.1 224.0.0.255 ==> IP Range Ban ==> Ban will be added/removed to IP Range ban list.

Please make sure exactly one whitespace between the two IP's.

1.3) IP in format e.g. 224.0.0.* ==> IP Range Ban ==> which is equal to 224.0.0.0 224.0.0.255 ==> Ban will be added/removed to IP Range ban list

2) If the Gploginpw password is too short (below 3 chars) the default password will be set which is: thepw

3) Rcon commands are NOT case sensitive, so you if you write GpBanIP or gpbanip is the same.

4) There has to be between rcon and the command exactly one whitespace.

5) If you use different passwords for GsProtector Rcon and your Server Rcon you need to set the password each time with rconpassword if you switch between commands e.g. rcon status (for the gameserver) and rcon gpstatus (for GsProtector)

Flood Testing

modder has provided a page where you can test if your game server is vulnerable to floods (rconpassword required):

<http://x-null.net/getstatus/getstatus.php>

For the testing, enable logging of your game server so that it prints query requests to the logfile, start then with the testing, if you find all of the 100 queries in your logfile your server is vulnerable to flooding attacks.

Credits:

modder,

members of TMT (www.modtheater.com),

AAAA (www.mohaaaa.co.uk),

Armageddon (www.crazygamersclan.com)

Mad Max (www.cipclan.com),

xnull (www.x-null.net)

Green <http://www.agb-clan.com>

GsProtector FAQ (Frequently asked Questions)

Q: Does this also work for Linux ?

A: No, this is only for Windows

Q: What's the limit on blocking a connection?

A: Every query that comes in quicker than 50ms = 20 queries per second is considered as attac

Q: If there is an attack and getstatus query is blocked does this prevent connecting to the server as well?

A: Players can still connect to the game server and play when there is an attac, except if a player is also attacker.

Q: Will there be a version for Linux Servers ?

A: Yes, if the final version for Windows is ready a version for Linux will be developed.

Q: Does this work for other games ?

A: No, currently this works only for mohaa, mohsh, mohbt games. But once the final version is realeasd I will develop versions for other games requested.