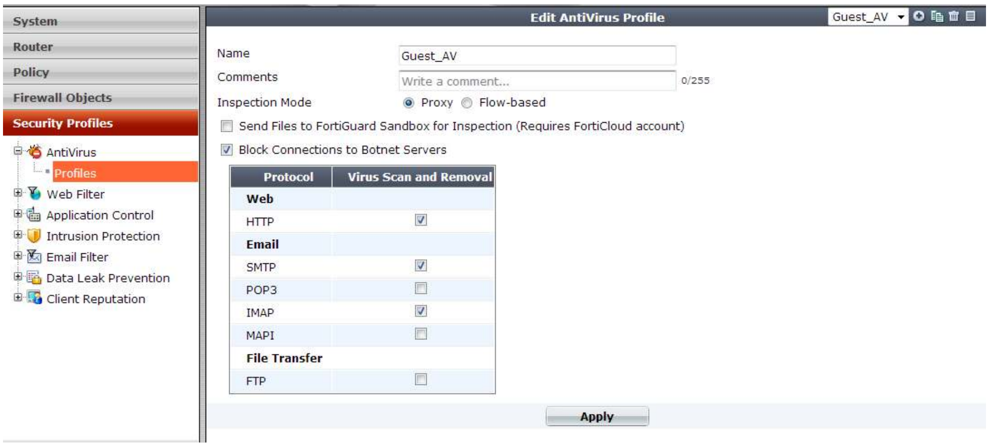
Configuration optimization for units with 512MB of RAM running FortiOS 5.0 or 5.2

Description	This article will help you optimize your configuration for older units with 512MB of RAM to work efficiently with FortiOS 5.0 and FortiOS 5.2.
Components	40C, 60C, 80C, 100C older revision with 512MB of ram

Identifying available memory	Connect to device CLI via console/ssh/telnet and issue following command
	`get hardware status`
	Following output is displayed:
	`Model name: FortiWiFi-60C`
	`ASIC version: CP0`
	`ASIC SRAM: 64M`
	`CPU: FortiSOC`
	`Number of CPUs: 1`
	`RAM: 436 MB`
	`Compact Flash: 7669 MB /dev/sda`
	`Hard disk: 7640 MB /dev/sda`
	`USB Flash: not available`
	`WiFi Chipset: Atheros AR5416`
	`WiFi firmware version: 0.9.17.1`
	On this particular hardware as you can see, 436MB of RAM is on disposal for FortiOS and 64MB has been pre-allocated for ASIC.
	FortiOS 5.0 and 5.2 have bigger foot print on memory usage, therefore units that have UTM features enabled with default settings, need to be optimized in order to lower memory usage. There are more new features in FortiOS 5.0 and 5.2 and if they are strictly not required in production, it is highly recommended to disable such features. Each function/feature requires CPU power and may have important memory foot print like: AntiVirus, IPS, AntiSpam, WebFiltering, Application Control, DDoS, Explicit Proxy …
	If your system memory usage is constantly high, or from time to time the system is entering conserve mode, and the output value for **RAM** as shown above is lower than **1009MB**, the following configuration changes may be required:
	• **Disable logging to memory, use FortiAnalyser or FortiCloud instead if logging is requirement**
	• **Disable unused protocols (HTTP, FTP, SMTP, POP3, IMAP, MAPI) from being antivirus scanned (Security Profiles> AntiVirus >Profiles)**

	- **Lower limit for oversized Files/Email inspection for all protocols** - **Lower limit for uncompressed file size** - **Lower compressed file size nesting level** - **Disable unnecessary IPS attack signatures** - **For DLP avoid using Content_Archive and if possible Content_summary (even when logging to FortiAnalyzer/FortiCloud, memory will be allocated for buffers)** - **Change session default timers for UDP and TCP** - **Disable the DHCP server if it is not required**

Disabling logging to memory	`config log memory setting`
	`set status disable`
	`end`
	
	Important NOTE: Do NOT enable disk logging, in 5.2 this feature is disabled, in 5.0 you will get warning message:
	"Enabling disk logging on this FortiGate unit will impact overall performance and reduce the lifetime of the unit. Fortinet recommends logging to FortiCloud."
	
	It is recommended to disable logging on non essential policies (policies for DNS traffic)

Disable unused protocols for AV inspection	From GUI you can uncheck protocols for AV inspection if you are not using those in your network, navigate from Security Profiles > AntiVirus >Profiles and select the AV profile you want to modify.  System Router Policy Firewall Objects Security Profiles AntiVirus Profiles Web Filter Application Control Intrusion Protection Email Filter Data Leak Prevention Client Reputation Edit AntiVirus Profile Apply Guest_AV Name Guest_AV Comments Write a comment... 0/255 Inspection Mode ● Proxy ○ Flow-based □ Send Files to FortiGuard Sandbox for Inspection (Requires FortiCloud account) ☑ Block Connections to Botnet Servers Protocol — Virus Scan and Removal **Web** HTTP ☑ **Email** SMTP ☑ POP3 □ IMAP ☑ MAPI □ **File Transfer** FTP □ You can also switch to Flow-based inspection which is less memory and cpu intensive, for more details please refer to online documentation http://docs.fortinet.com
Changing the	Proxy options provides you with the possibility to apply a maximum in-

<table>
<tr>
<td>maximum allowed file size</td>
<td>

memory file size that will be scanned, in megabytes, for each of the network protocols (ftp, http, im, imap, nntp, mapi, pop3 or smtp) in the profile.

If the file is larger than the oversize-limit, the file is passed or blocked, depending on whether "oversize" is a selected <service> option (See example below).
When "oversize" is a configured option, files that are over the file size limit are blocked.

```
config firewall profile-protocol-options
edit <profile>
config <service>
set oversize-limit 2
```

Where:

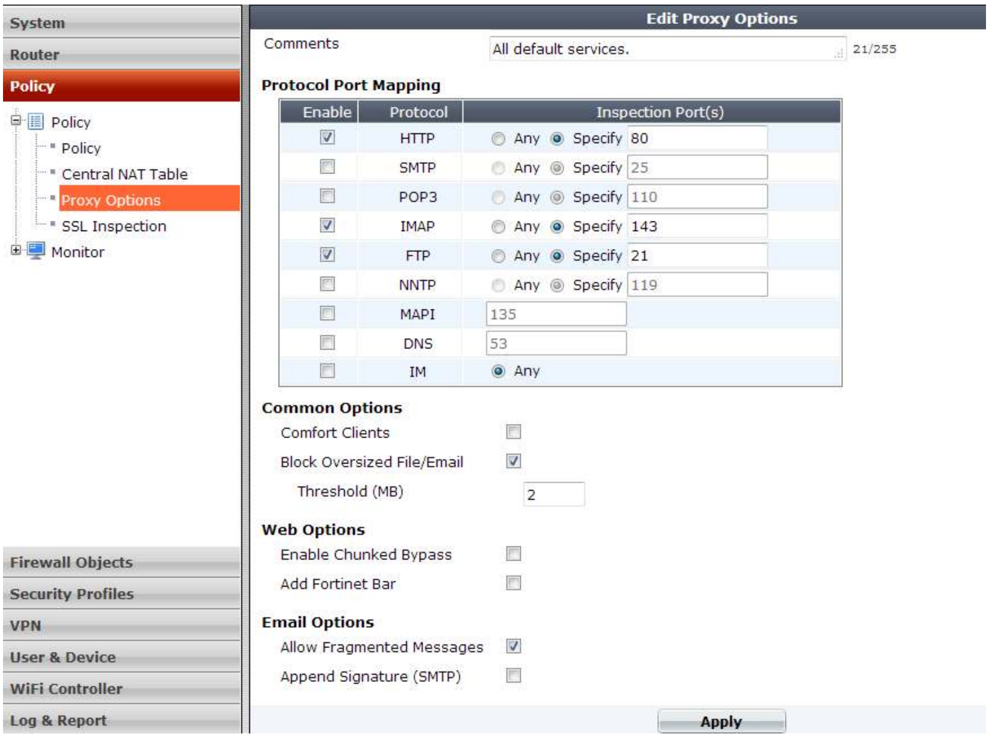
```
<service> is ftp, http, im, imap, nntp, mapi, pop3 or smtp.
<profile> could be a custom profile, or the default one.
```

Recommended value for AV profile would inspect only http, ftp and imap traffic that is 2MB or less, you can chose either to pass oversized files or to block them.

```
config firewall profile-protocol-options

edit "Guest_proto"
        set extended-utm-log enable
            config http
                set ports 80
                set options oversize no-content-summary
                set comfort-interval 3
                set comfort-amount 64
                unset post-lang
                set oversize-limit 2
            end
            config ftp
                set ports 21
                set options oversize no-content-summary
                set comfort-interval 3
                set comfort-amount 64
                set oversize-limit 2
            end
            config imap
                set ports 143
                set options fragmail oversize no-content-
summary
                set oversize-limit 2
            end
next
end
```

</td>
</tr>
</table>



Edit Proxy Options

Comments: All default services. 21/255

Protocol Port Mapping

Enable	Protocol	Inspection Port(s)
☑	HTTP	○ Any ● Specify 80
□	SMTP	○ Any ● Specify 25
□	POP3	○ Any ● Specify 110
☑	IMAP	○ Any ● Specify 143
☑	FTP	○ Any ● Specify 21
□	NNTP	○ Any ● Specify 119
□	MAPI	135
□	DNS	53
□	IM	● Any

Common Options

Comfort Clients □

Block Oversized File/Email ☑

Threshold (MB) 2

Web Options

Enable Chunked Bypass □

Add Fortinet Bar □

Email Options

Allow Fragmented Messages ☑

Append Signature (SMTP) □

Changing the uncompressed file size limit (scan buffer size)

From the FortiOS v4.3, v5.0 and v5.2.0 CLI, you can use the "config antivirus service" command to control the maximum file size that can be buffered before virus scanning. Files bigger than this value are passed without scanning. Note however that archived files are first extracted before being compared to the scan buffer size. Likewise, email attachments are decoded

You can set the uncompressed file size limit for each service as follows.

In FortiOS v5.0 and v5.2.0

```
config antivirus service <service>
    set uncompsizelimit <MB_integer>
end
```

In FortiOS v5.2.1

```
config firewall profile-protocol-options
 edit <profile>
  config <service>
   set uncompressed-oversize-limit <MB_integer>
end
```

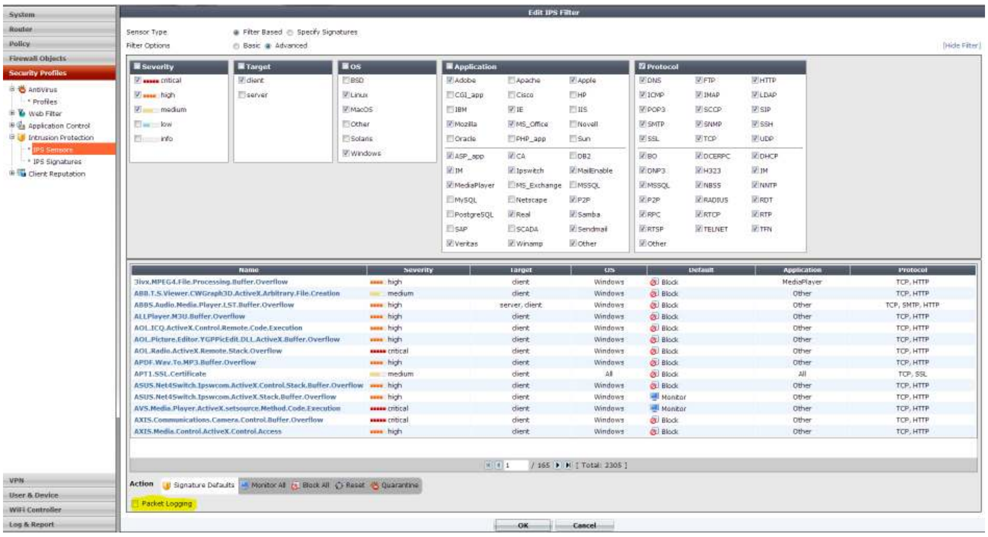
Where:

	<service> ftp, http, im, imap, nntp, mapi, pop3, smtp, https, imaps, pop3s, smtps, or ftps. <profile> could be a custom profile, or the default one. <MB_integer> can be from 0 to the maximum oversize threshold. Enter "set uncompsizelimit?" to display the buffer size range for your FortiGate unit. Recommended value for low end units is 1- 3MB.

Changing the compressed file nesting level (archive scan depth)	From the FortiOS v5.0 and v5.2.0 CLI, you can use the "config antivirus service" command to control the number of compression levels that FortiOS will open before virus scanning the resulting uncompressed file. You can set the number of levels for each service.
	
	FortiOS v5.0 and v5.2.0
	`config antivirus service <service>`
	`set uncompnestlimit <depth_integer>`
	`end`
	
	In FortiOS v5.2.1
	`config firewall profile-protocol-options`
	`edit <profile>`
	`config <service>`
	`set set uncompressed-nest-limit <depth_integer>`
	`end`
	
	Where:
	
	<service> ftp, http, im, imap, nntp, mapi, pop3, smtp, https, imaps, pop3s, smtps, or ftps.
	<profile> could be a custom profile, or the default one.
	<depth_integer> can be from 2 to 100.
	
	Recommended value on small end units is for uncompressed-nest-limit is 2-3.

Disable unnecessary IPS attack signatures	Disable any IPS attack signature that you are certain it is not being in used. Additionally its highly recommended not to use packet logging when a signature match is found. e.g. If you don’t have any servers in your network, than selecting protection for clients will be sufficient for your use. If you only using Windows and MAC OS systems for example, select only signatures for those. The same is valid with known protocols and applications. In order to do this you need to navigate from the web GUI:

Security Profiles > Intrusion Protection > IPS Sensors



Edit IPS Filter

Sensor Type ● Filter Based ○ Specify Signatures

Filter Options ○ Basic ● Advanced

[Hide Filter]

Severity: ☑ critical ☑ high ☑ medium □ low □ info

Target: ☑ client □ server

OS: □ BSD ☑ Linux ☑ MacOS □ Other □ Solaris ☑ Windows

Application: ☑ Adobe □ Apache ☑ Apple □ CGI_app □ Cisco □ HP □ IBM ☑ IE □ IIS ☑ Mozilla ☑ MS_Office □ Novell □ Oracle □ PHP_app □ Sun ☑ ASP_app ☑ CA □ DB2 ☑ IM ☑ Ipswitch ☑ MailEnable ☑ MediaPlayer □ MS_Exchange □ MSSQL □ MySQL □ Netscape ☑ P2P □ PostgreSQL ☑ Real ☑ Samba □ SAP □ SCADA ☑ Sendmail ☑ Veritas ☑ Winamp ☑ Other

☑ Protocol: ☑ DNS ☑ FTP ☑ HTTP ☑ ICMP ☑ IMAP ☑ LDAP ☑ POP3 ☑ SCCP ☑ SIP ☑ SMTP ☑ SNMP ☑ SSH ☑ SSL ☑ TCP ☑ UDP ☑ BO ☑ DCERPC ☑ DHCP ☑ DNP3 ☑ H323 ☑ IM ☑ MSSQL ☑ NBSS ☑ NNTP ☑ P2P ☑ RADIUS ☑ RDT ☑ RPC ☑ RTCP ☑ RTP ☑ RTSP ☑ TELNET ☑ TFN ☑ Other

Name	Severity	Target	OS	Default	Application	Protocol
3ivx.MPEG4.File.Processing.Buffer.Overflow	high	client	Windows	Block	MediaPlayer	TCP, HTTP
ABB.T.S.Viewer.CWGraph3D.ActiveX.Arbitrary.File.Creation	medium	client	Windows	Block	Other	TCP, HTTP
ABBS.Audio.Media.Player.LST.Buffer.Overflow	high	server, client	Windows	Block	Other	TCP, SMTP, HTTP
ALLPlayer.M3U.Buffer.Overflow	high	client	Windows	Block	Other	TCP, HTTP
AOL.ICQ.ActiveX.Control.Remote.Code.Execution	high	client	Windows	Block	Other	TCP, HTTP
AOL.Picture.Editor.YGPPicEdit.DLL.ActiveX.Buffer.Overflow	high	client	Windows	Block	Other	TCP, HTTP
AOL.Radio.ActiveX.Remote.Stack.Overflow	critical	client	Windows	Block	Other	TCP, HTTP
APDF.Wav.To.MP3.Buffer.Overflow	high	client	Windows	Block	Other	TCP, HTTP
APT1.SSL.Certificate	medium	client	All	Block	All	TCP, SSL
ASUS.Net4Switch.Ipswcom.ActiveX.Control.Stack.Buffer.Overflow	high	client	Windows	Block	Other	TCP, HTTP
ASUS.Net4Switch.Ipswcom.ActiveX.Stack.Buffer.Overflow	high	client	Windows	Monitor	Other	TCP, HTTP
AVS.Media.Player.ActiveX.setsource.Method.Code.Execution	critical	client	Windows	Monitor	Other	TCP, HTTP
AXIS.Communications.Camera.Control.Buffer.Overflow	critical	client	Windows	Block	Other	TCP, HTTP
AXIS.Media.Control.ActiveX.Control.Access	high	client	Windows	Block	Other	TCP, HTTP

1 / 165 [Total: 2305]

Action: Signature Defaults | Monitor All | Block All | Reset | Quarantine

□ Packet Logging

OK Cancel

It is highly recommended to change the algorithm for IPS engines on units with 512MB of ram, this can be done through CLI:

```
config ips global
set algorithm low
end
```

Session Timers

Change the default session TTL:

```
config system session-ttl
   set default 300
end
```

You may have a requirement for particular traffic to have a longer idle timeout for the session, this can be configured in the CLI under the firewall policy allowing such flows longer session TTL’s:

```
config firewall policy
edit xxx
set session-ttl 3600 (you can define time in seconds)
end
```

```
config system global
    set tcp-halfclose-timer 30
    set tcp-halfopen-timer 10
    set tcp-timewait-timer 1
    set udp-idle-timer 60
```

```
end
```

Change the FortiGuard TTL

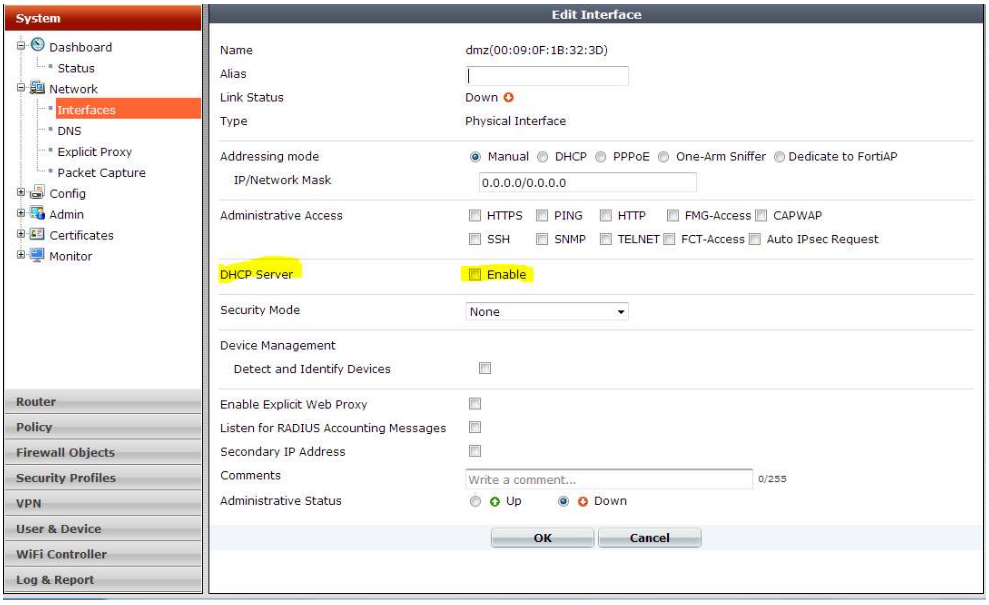
```
config system fortiguard
   set webfilter-cache-ttl 500
   set antispam-cache-ttl 500
end
```

Change DNS cache:

```
config system dns
   set dns-cache-limit 300
end
```

Disable unused DHCP servers

From GUI navigate System >Network> Interfaces and uncheck DHCP Server box on interfaces where this is not used or required, see bellow:



Name: dmz(00:09:0F:1B:32:3D)

Alias:

Link Status: Down

Type: Physical Interface

Addressing mode: ● Manual ○ DHCP ○ PPPoE ○ One-Arm Sniffer ○ Dedicate to FortiAP

IP/Network Mask: 0.0.0.0/0.0.0.0

Administrative Access: □ HTTPS □ PING □ HTTP □ FMG-Access □ CAPWAP □ SSH □ SNMP □ TELNET □ FCT-Access □ Auto IPsec Request

DHCP Server: □ Enable

Security Mode: None

Device Management

Detect and Identify Devices □

Enable Explicit Web Proxy □

Listen for RADIUS Accounting Messages □

Secondary IP Address □

Comments: Write a comment... 0/255

Administrative Status: ○ Up ● Down