How to troubleshoot issues with viruses that seem to pass through the Fortigate – v2.80
Feb. 9, 2004.
Updated May 3, 2004; Sept. 7, 2004; Feb. 16, 2005. Mar. 29, 2005.

This is an unofficial Fortinet documentation written and/or compiled by Fortinet's EMEA support center eu_support@fortinet.com . It's a How-To guide with the purpose of providing complementary information to our customers on configuring or troubleshooting Fortigate units and/or 3rd party products that interact with the Fortigate. We have done our best to confirm the accuracy and validity of this guide, but it is possible that errors may exist.

Official Fortinet documentation is available at:
ftp://pftp:FortiOS@support.fortinet.com/ and http://kc.forticare.com

//----------//

This document applies to FortiOS v2.80 due to the CLI and GUI references, but the same procedure could essentially be applied on a v2.36 or v2.50 unit.

Please check the following and follow the suggested actions:

1) Virus signature versions and update configuration:

Your virus signatures may not be up to date. You can verify your current anti-virus version in the GUI (System->Status) or (System->Maintenance->Update Center)
- Compare your version to the current version displayed at http://www.fortinet.com/FortiProtectCenter/

If your virus signatures are not up to date, please proceed with a manual signature update (System->Maintenance->Update Center), and also review your automatic update configuration settings.

You will find detailed information concerning this procedure, in the Fortigate Installation and Configuration guide.

Note:
If your Anti-Virus and Attack Definitions are displayed as version(s) "0.00", please contact Fortinet support for further instructions on how to correct this problem.

2) Cases when the Fortigate cannot detect viruses :

a) If the traffic doesn't go through the FortiGate, it can't be scanned.

Verify that there is no other access to your network (example: a secondary backup gateway).
Other 'bypass' methods can be:
- users with laptops who bring viruses from their home internet connection.
- other non protected Internet links such as analog modem dial-up connections, an open WiFi network or rogue WiFi device, or other VPNs gateways.

b) If the virus is received in a password protected zip (or other compressed) file, the Fortigate is unable to open the compressed file, and is therefore unable to scan it. This can be presented as a type of "social hacking", where the user who receives the password protected zip file, is asked to open it with the provided password in an email, in the hope of releasing the virus.

c) If the virus is received through an encrypted connection, the Fortigate cannot scan it:

- Certain web-mail services use HTTPS.
- SMTP mail servers may be configured to negotiate an encrypted exchange using TLS.

d) If the connection port used, is not the standard protocol port :
The Fortigate can scan other ports besides the standard 25 (SMTP), 80 (HTTP), 110 (POP3), and 143 (IMAP), but they must be configured via the CLI command, as shown below:

conf antivirus service <protocol>

HTTP proxied connections can also be scanned, by configuring the proxy port for the HTTP protocol (see example above).

e) FortiGate configuration error(s) :

Verify the FortiGate firewall policies that protect your network against viruses, and check that:

- The "Protection Profile" checkbox is enabled.
- The proper Protection Profile is selected.

Review your Protection Profiles (Firewall->Protection Profile) and make sure that you have enabled "Anti-Virus Virus Scan" for the needed protocols.

Is Firewall->Protection Profile->Anti-Virus->"Oversized File/Email" set to "Pass" ? If so, then any attachments/files of size greater than the values specified in Anti-Virus->Config->Config , will not be scanned and will pass through.

3) The effects of SMTP "splice" feature and false-positive detection by A/V software running on mail servers.

The Fortigate's "splice" feature improves A/V scan performance by simultanously scanning an incoming email and transfering it to the mail server. Should a virus be detected, the data transfer which was started to the SMTP server will be aborted with a 554 SMTP error code. Under certain circumstances, an A/V software that is running on this SMTP server, may have already received sufficient data to determine that it contained a virus, and raise an alert. Normally this email will not have been delivered to the receiving user, since it was terminated by the sending server (in this case the Fortigate unit), and the SMTP server would have also discarded the incomplete transmission. Additional information on SMTP "splice" behavior, is available in the following Knowledge Base article:
http://kc.forticare.com/default.asp?id=662&Lang=1

4) If the cause has been verified as not being one of the above, please provide us with:

a) A network diagram (with IP subnets and addresses), showing :
- the hosts that detected (or were infected) by the virus.
- the type and version of mail server used, with details concerning its configuration (example: POP3, IMAP, incoming SMTP, outgoing SMTP)

b) Details on the connection path that may have introduced the virus.

Example:

- Mail sent from user@company.com to user@mycompany.com
- arrived at the Fortigate VIP on external interface with IP 195.115.32.12 on port 25, forwarded to internal SMTP server at IP 192.168.1.1
- Fortigate firewall external->interal policy ID 5 matched, with AV enable, and Protection Profile set to "Strict"

c) A password protected zip file, containing the detected virus. Use the password ‘fortinet’ for the zip file.

d) The Fortigate Attack and Anti-Virus log files:
- alog.log (Log&Report->Log Access->Attack Log)
- vlog.log (Log&Report->Log Access->Anti-Virus Log)

e) The following CLI commands output :

```
conf sys con
set outp stan
end
get sys stat
get sys perf
diag sys matr
diag hard sys mem
diag sys auto stat
diag sys auto ver
get sys auto over
get sys auto push
get sys auto sche
get sys auto tun
diag sys sess stat
diag netl dev list
diag netl int list
diag hard dev nic internal
diag hard dev nic external
diag hard dev nic dmz
diag hard dev nic ha
diag hard dev nic wan1
diag hard dev nic wan2
diag hard dev nic port1
....etc...
diag netl ip list
diag netl neighbor list
get sys int
get sys int internal
get sys int external
get sys int dmz
get sys int ha
get sys int wan1
get sys int wan2
get sys int port1
....etc...
get rout info routing
diag netl route list
diag test update info
show
```

Looking for information on viruses/threats/worms ?

Please use our encyclopedia and search engine at http://www.fortinet.com/FortiProtectCenter/

Fortinet documentation:

All of our documentation is available on our FTP server and in our Knowledge Center:

FTP site : support.fortinet.com
login : pftp
passwd : FortiOS

directory v2.80/v2.80_doc

Fortinet Knowledge Center:
http://kc.forticare.com