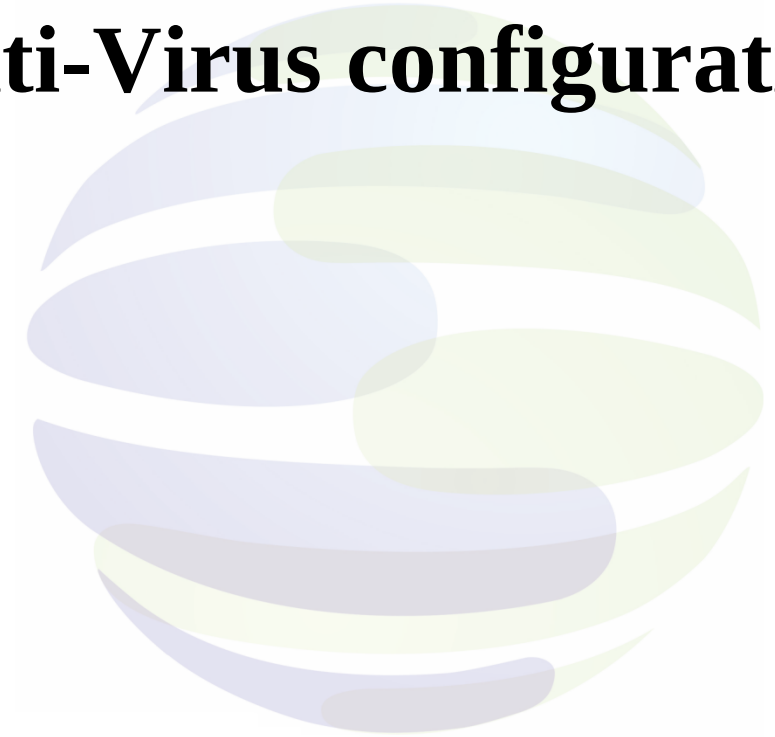
SANGFOR_NGAF_v7.4_
Anti-Virus configuration



SANGFOR Technologies Inc.

4/1/2018

Your Future-Proof IT Enabler

Sangfor Technologies

Block A1, Nanshan iPark, No.1001 Xueyuan Road,Nanshan District, Shenzhen, China

T.: +60 12711 7129 (7511) | E.: tech.support@sangfor.com | W.: www.sangfor.com

Declaration

Copyright © SANGFOR Technologies Inc. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.

SANGFOR, SINFOR and logo are the trademarks of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective holders.

Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

The information in this document is subject to change without notice.

To obtain the latest version, contact the international service center of SANGFOR Technologies Inc.

Sangfor Technologies

Block A1, Nanshan iPark, No.1001 Xueyuan Road,Nanshan District, Shenzhen, China

T.: +60 12711 7129 (7511) | E.: tech.support@sangfor.com | W.: www.sangfor.com

Table of contents

Sangfor Technologies
Block A1, Nanshan iPark, No.1001 Xueyuan Road,Nanshan District, Shenzhen, China
T.: +60 12711 7129 (7511) | E.: tech.support@sangfor.com | W.: www.sangfor.com

1 Introduction

1.1 Abbreviations and conventions

AC in this article refers to the SANGFOR AC device.

1.2 Feedback

If you find any questions of this documents, please feel free to give us feedback, email: tech.support@sangfor.com.

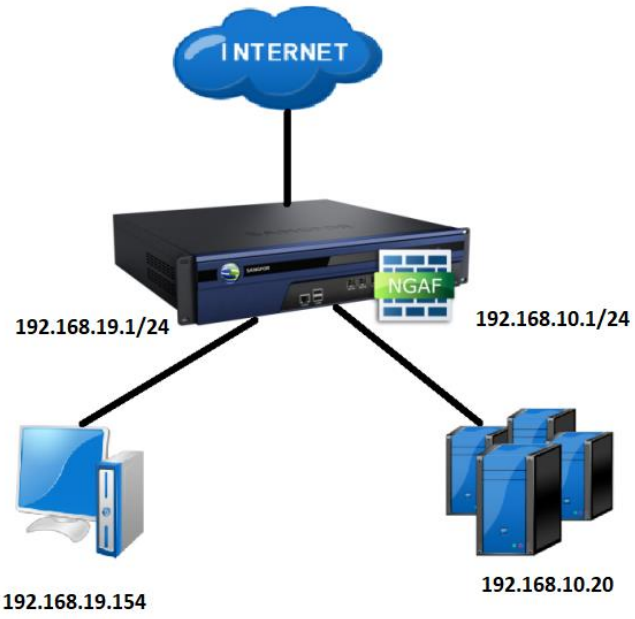
2 Introduction of Anti-Virus feature

Internal users are able to receive virus file through HTTP, mailing address and etc. Sangfor NGAF Content Security module is to against this kind of problem. This module able to detect and kill the virus, protect internal users from viruses and harassment. In the same time, it is able to improve an organization's network security and record deny logs for tracking and analysis.

3 Test scenario

3.1 Test diagram

Anti-Virus scenario:



Internal users will inadvertently download and upload virus files via http and email. When the traffic contains virus file and pass through NGAF will been identified. NGAF will deny and logs the packet according to the policies which set by users.

4 Important Requirement

i. The Multi-Function license in NGAF device must enabled “Anti-Virus” and license of “Anti-Virus Database”.

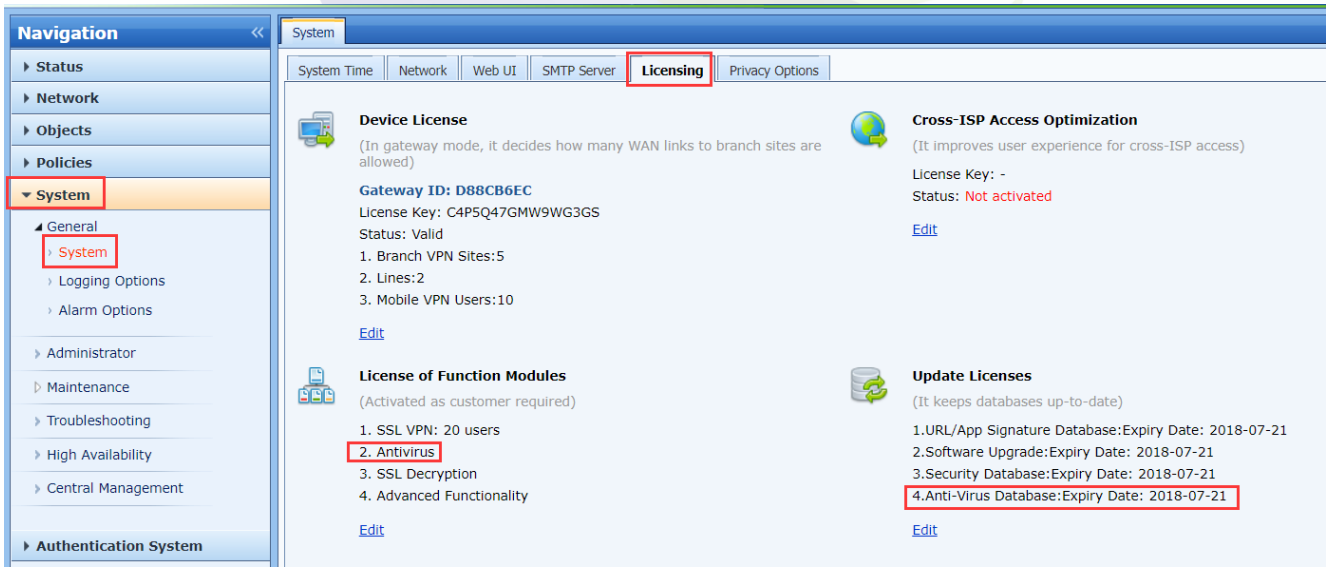
ii. The protected object’s traffic must go through the NGAF device. It does not support in bypass mode.

iii. Ensure the protection object’s traffic passes NGAF.

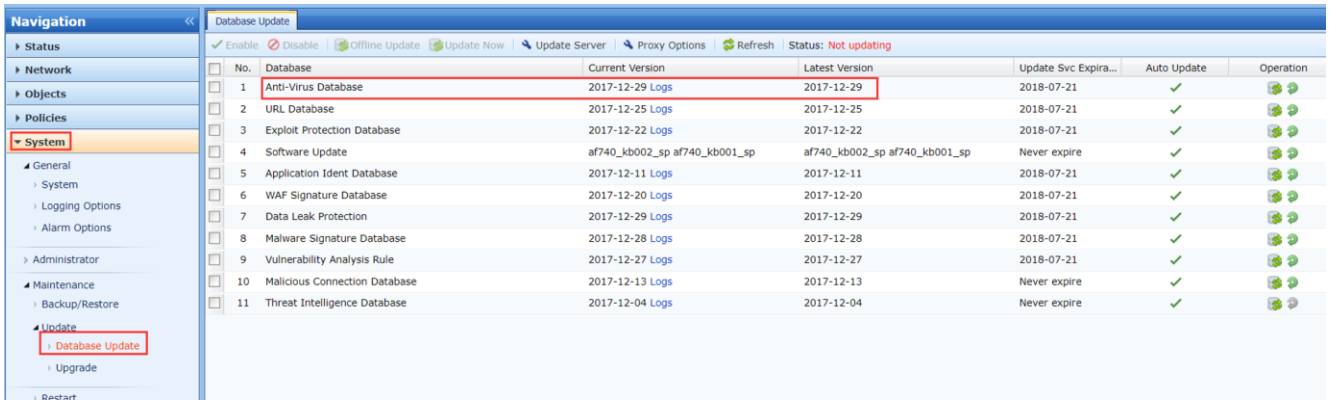
5 Configuration

5.1 Valid Authorization

5.1.1 First, ensure the NGAF device is having Anti-Virus function module and the license of anti-virus database, as shown below:

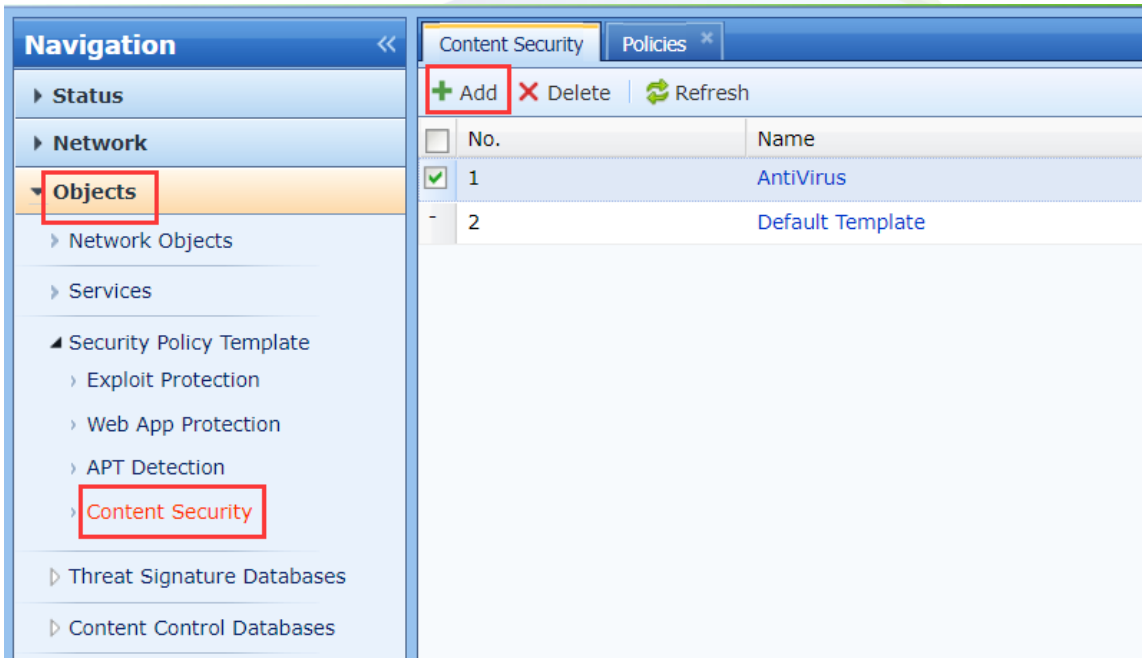


5.1.2 Then make sure the Anti-Virus database is up to date.

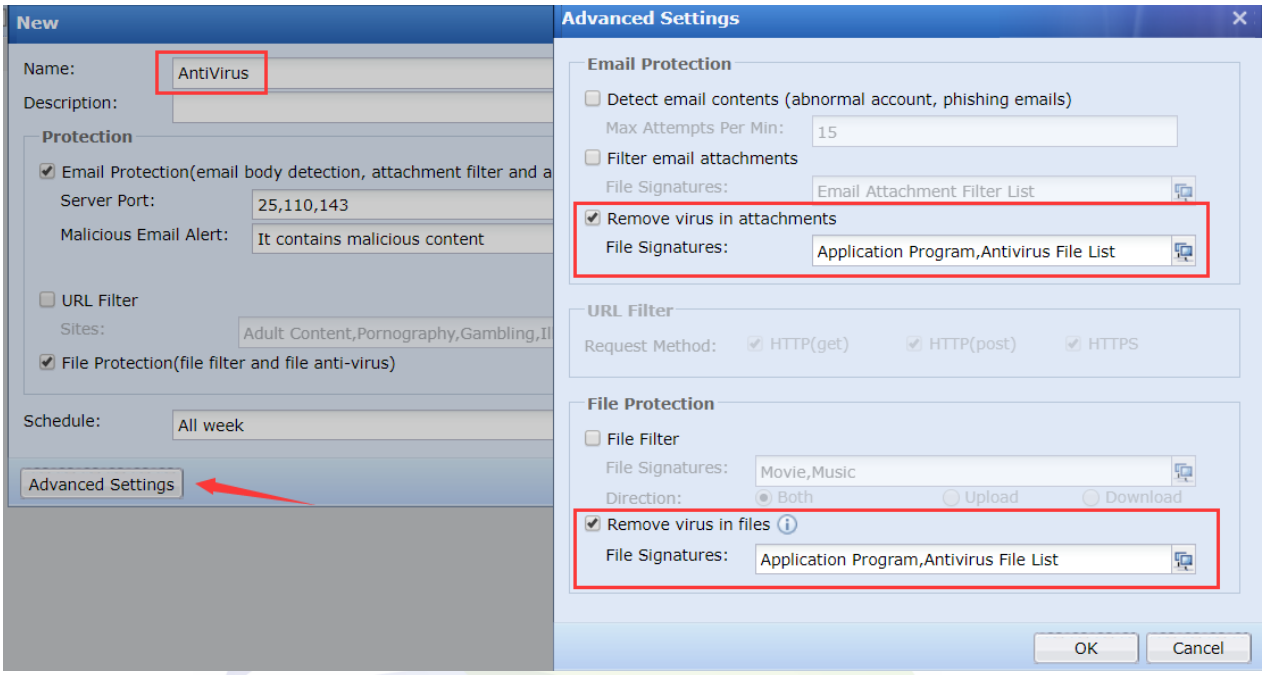


5.2 Configuration of Anti-Virus

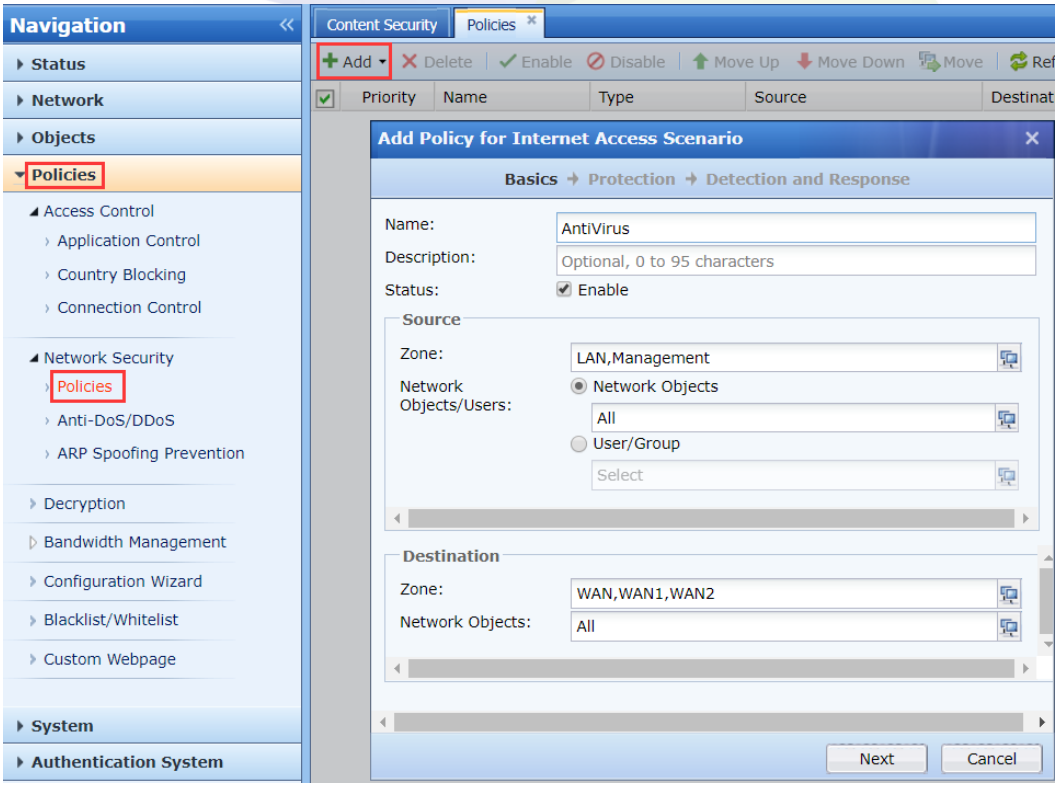
5.2.1 Click on the [Objects] - [Content Security] to enter the policy settings page, click Add



5.2.2 From New Template insert a name for the policy. The protection tick on the Email Protection and File Protection. The server port and malicious email alert leave it as default. After that click on the Advance Settings then tick on the Remove virus in attachments and Remove virus in files only. The File Signatures select Application Program, Anti-virus and File list.



5.2.3 Next, enter to the policies page which under network security. Click Add and fill in the policy name. Select LAN for Source Zone and WAN for Destination Zone. Both network objects/users select as All.

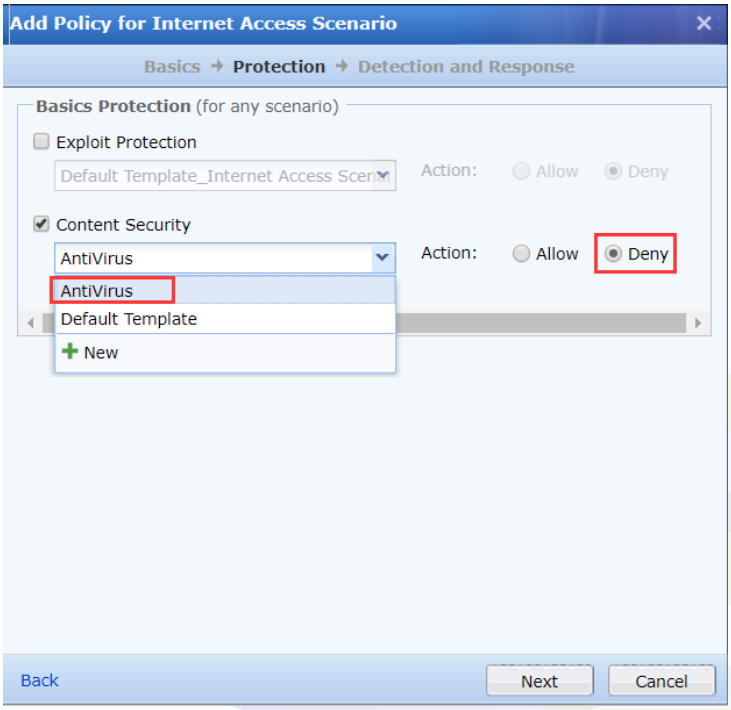


Sangfor Technologies

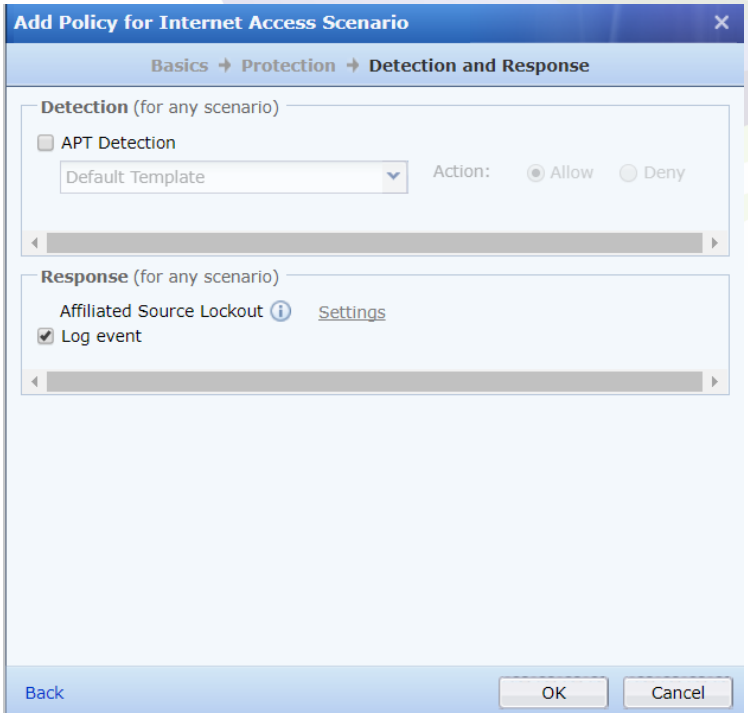
Block A1, Nanshan iPark, No.1001 Xueyuan Road,Nanshan District, Shenzhen, China

T.: +60 12711 7129 (7511) | E.: tech.support@sangfor.com | W.: www.sangfor.com

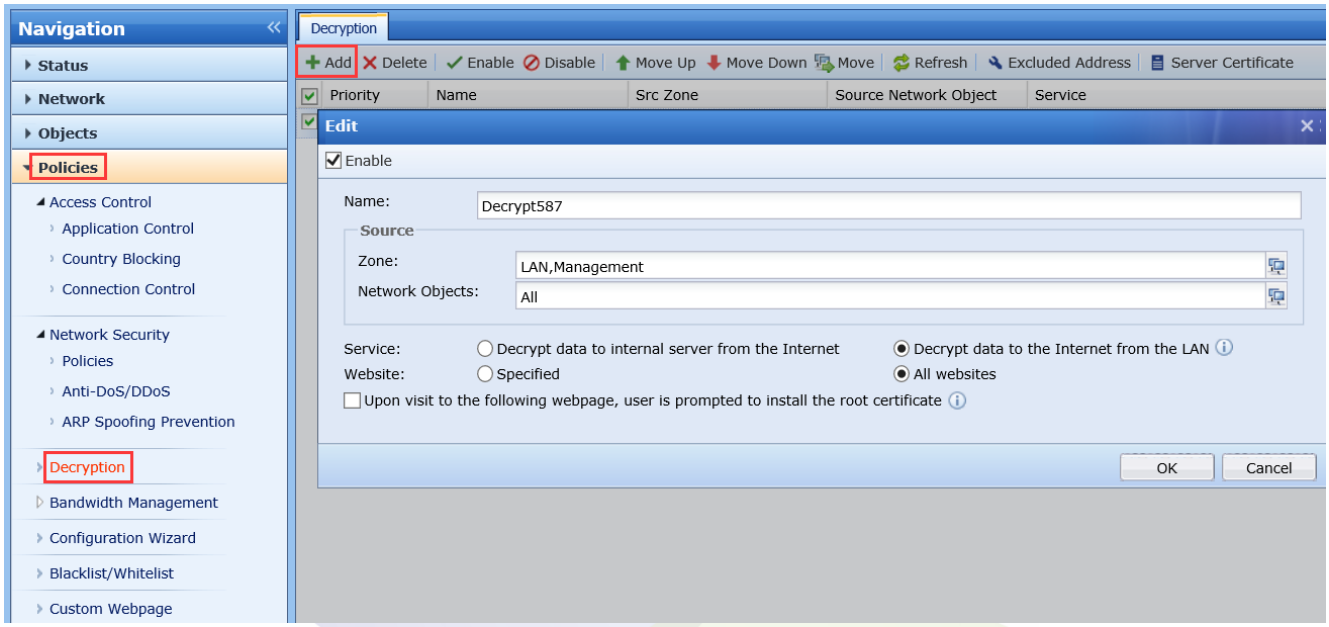
5.3.4 After that click on the “Next” button, just tick on the Content Security and select the Anti-Virus template which created in previous. Tick Deny for the action.



5.2.5 Click next again to the last stage. Untick the APT Detection and tick on the Log event to log the activity. Click Ok to finish.



5.2.6 Ensure enable decryption feature in NGAF if using SSL port to send email. Go to [Policies] - [Decryption] add a new decryption policy. Give a name to the policy, select LAN as source zone. Tick “decryption data to the Internet from the LAN” option and All websites. Lastly, click Ok to create the policy.

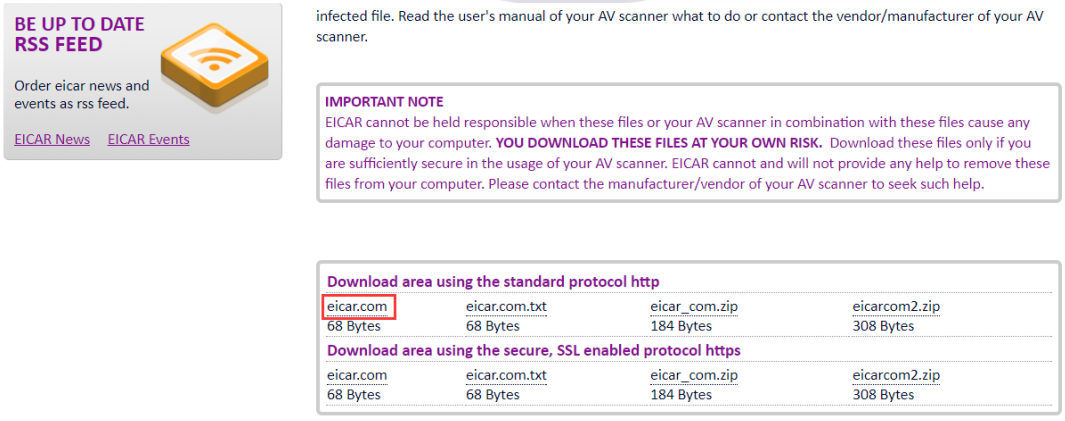


6 Anti-Virus function testing

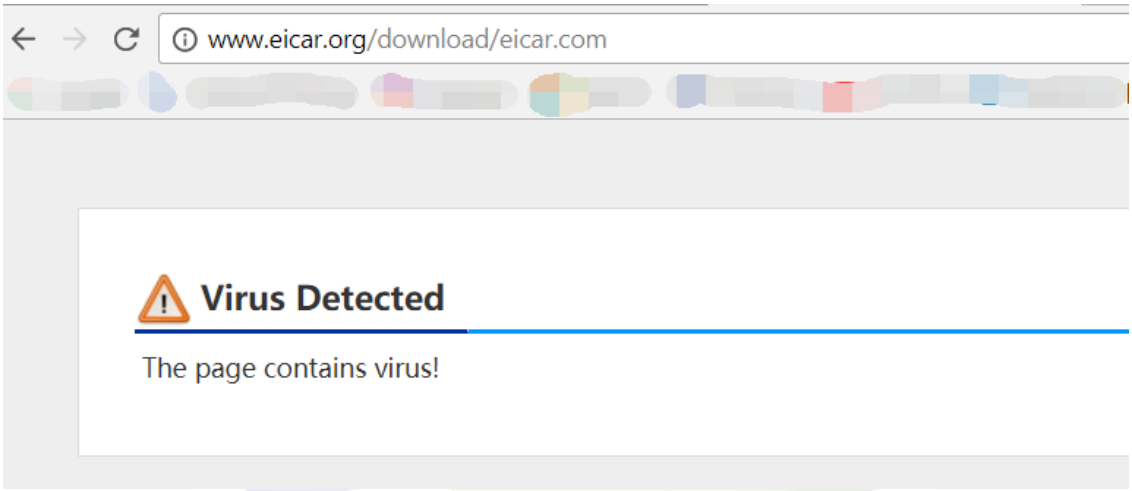
Now provide 2 testing methods for http download virus files and send email with virus attachment.

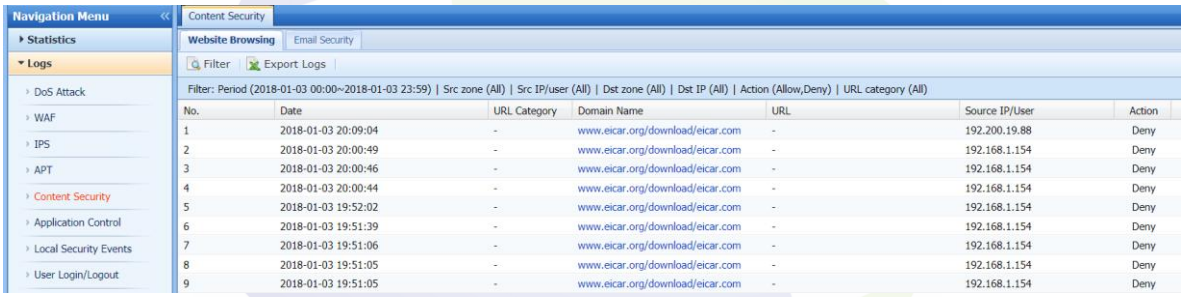
6.1 HTTP download virus file

6.1.1 Visit the website http://www.eicar.org/85-0-Download.html, right click on the eicar.com folder to download it.



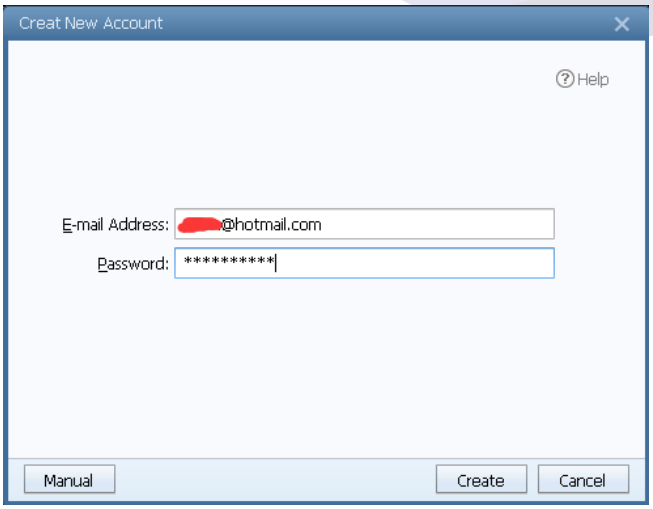
6.1.2 When the page shows Virus Detected message, enter to the internal data center you can see there is some Deny logs from [Logs] - [Content Security] - [Website Browsing]





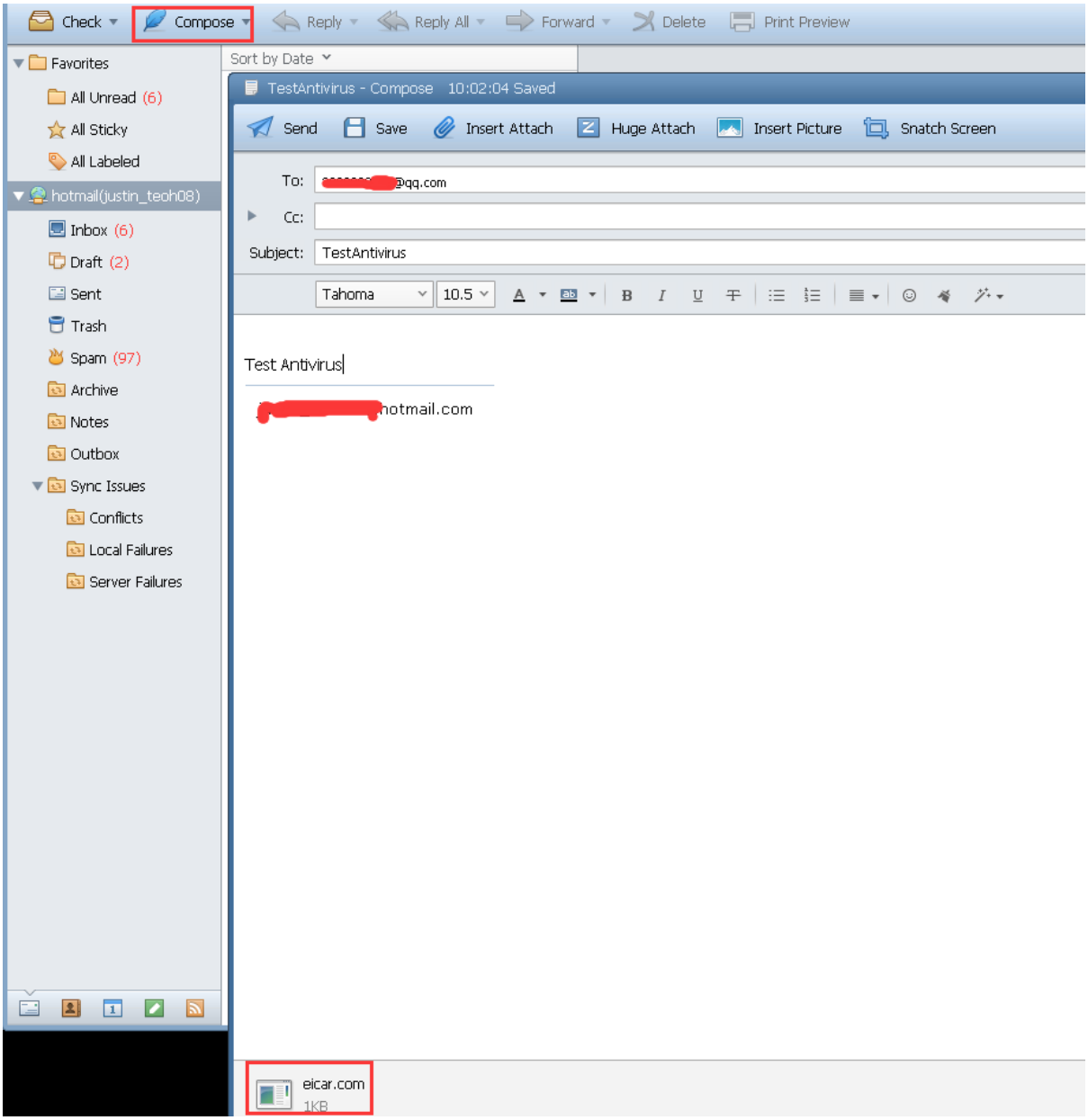
6.2 Send email with Virus attachment

6.2.1 Download and install the email client software - Foxmail. Fill in the email and password, then click Create button.

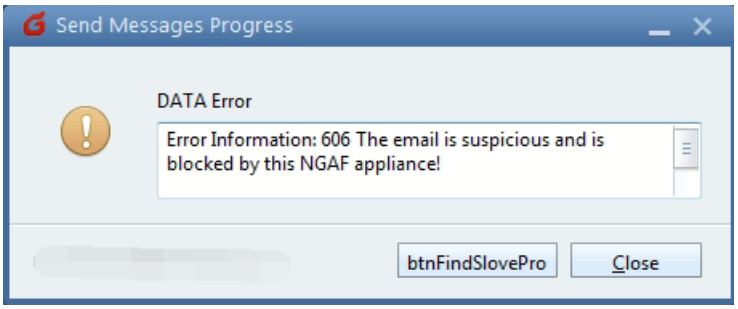


6.2.2 After login to Foxmail, click Compose and fill in the recipient, subject and content. Then click on the Insert attach button, attach eicar.com folder and send it.

***Note**: eicar.com folder must download before policy has been created. Download the eicar.com folder from http://www.eicar.org/85-0-Download.html. Do remember Save as to other location but not run it.



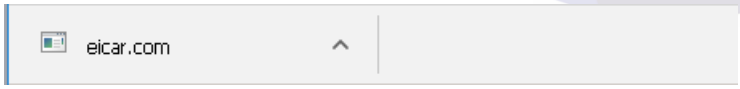
6.2.3 Foxmail shows error message: 606 The email is suspicious and is blocked by this NGAF appliance!



6.2.4 From NGAF internal data center, click on [Logs] - [Content Security] - [Email Security] can see the deny logs.

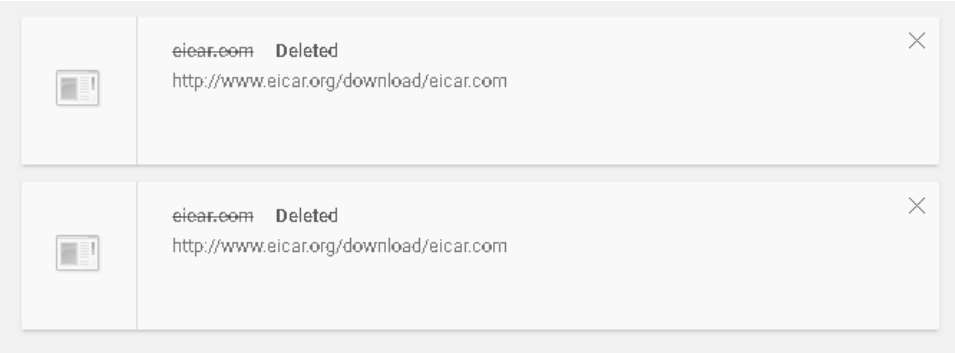
7 Attentions

1. Do remember not to run the eicar.com folder after downloaded, otherwise the PC has high chances affected by virus.

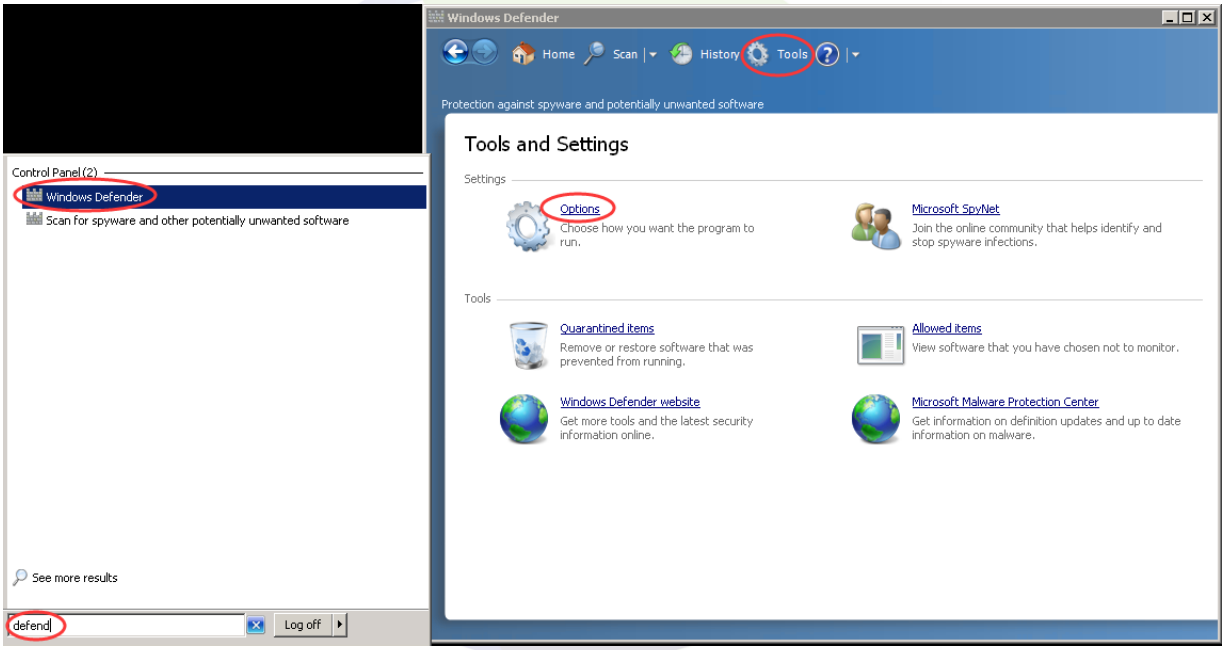


2. After finish testing, do remember delete the eicar.com folder from local.

3. Sometimes the pc running with windows will prompt the message as below if download the eicar.com folder from http://www.eicar.org/85-0-Download.html. This is due to windows system comes with security software - Windows Defender which use to kill and delete viruses. Kindly close the Windows Defender temporary for download eicar.com folder. Refer to the steps at below.



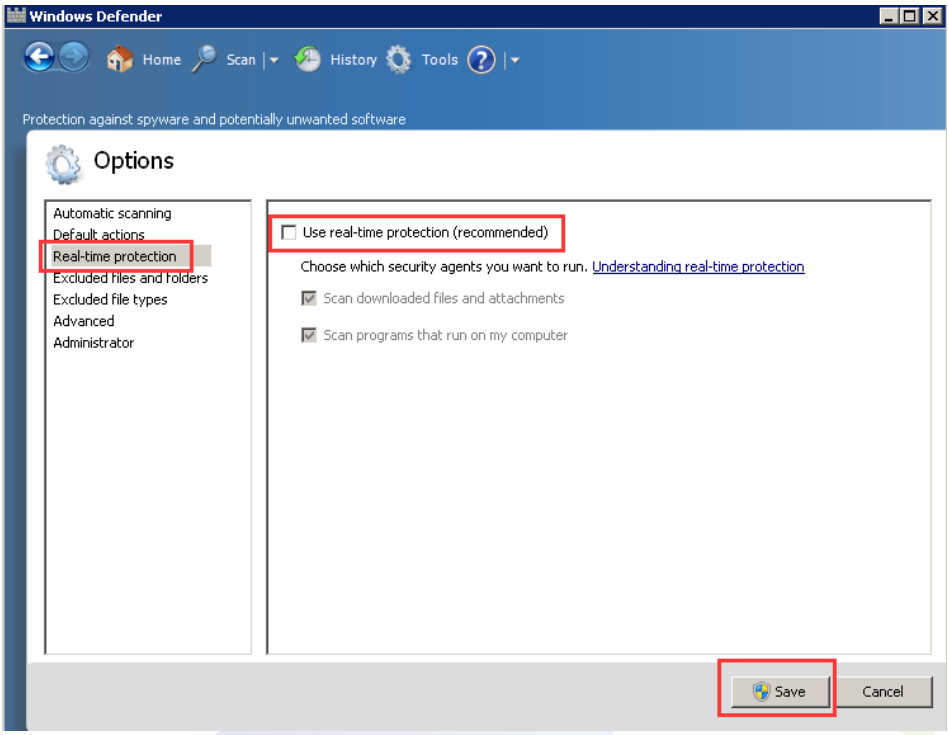
4. Click Start, search defender and open the Windows Defender. Select Tools, click Options from settings. After that click Real-time protection and disable “Use real-time protection”. Click Save to finish.



Sangfor Technologies

Block A1, Nanshan iPark, No.1001 Xueyuan Road,Nanshan District, Shenzhen, China

T.: +60 12711 7129 (7511) | E.: tech.support@sangfor.com | W.: www.sangfor.com



5. NGAF anti-virus does support SMTP, POP3 and IMAP protocol with non-encrypted and encrypted email with port 995, 465, 587 and so on. Kindly enable decryption feature in NGAF if using SSL port. (For decryption feature, kindly refer to user manual of decryption)

Sangfor Technologies

Block A1, Nanshan iPark, No.1001 Xueyuan Road,Nanshan District, Shenzhen, China

T.: +60 12711 7129 (7511) | E.: tech.support@sangfor.com | W.: www.sangfor.com