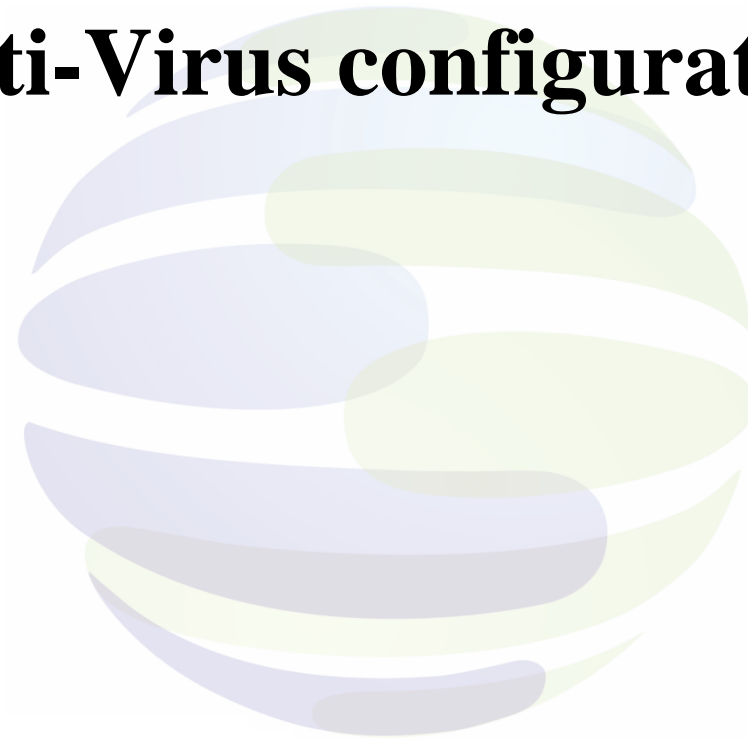




SANGFOR

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.: +86 755 2654 8888 (7511) | E.: tech.support@sangfor.com | W.: www.sangfor.com



Declaration

Copyright © SANGFOR Technologies Inc. All rights reserved.

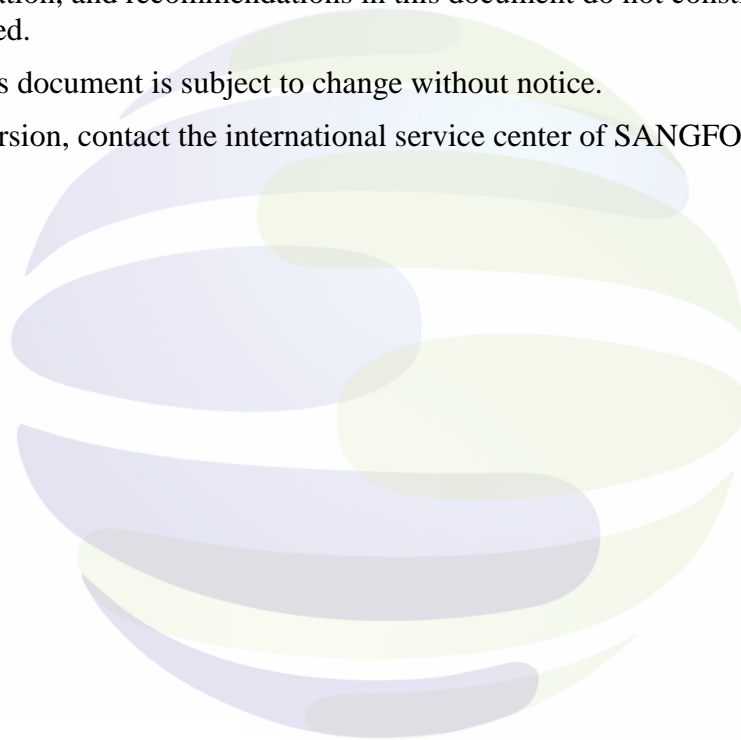
No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.

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.



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



Table of contents

Declaration	2
Table of contents	3
1 Introduction	4
1.1 Abbreviations and conventions	4
1.2 Feedback	4
2 Introduction of Anti-Virus feature	4
3 Test scenario	4
3.1 Test diagram	4
4 Important Requirement	5
5 Configuration	5
5.1 Valid Authorization	5
5.2 Configuration of Anti-Virus	6
6 Anti-Virus function testing	9
6.1 HTTP download virus file	9
6.2 Send email with Virus attachment	10
7 Attentions	12

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



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.

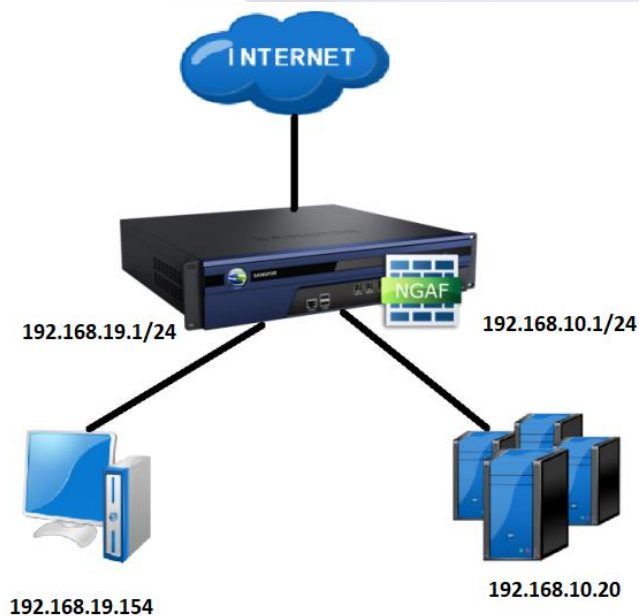
2 Introduction of Anti-Virus feature

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:



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



Internal users will inadvertently download and upload virus files via http and email. When the traffic contains virus file and pass through NGAF will be 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:

The screenshot displays the Sangfor NGAF web management interface. On the left, the 'Navigation' sidebar has the 'System' menu item selected. The main panel shows the 'Licensing' configuration page. It includes sections for 'Device License' (showing Gateway ID: D88CB6EC, License Key: C4P5Q47GMW9WG3GS, and Status: Valid), 'License of Function Modules' (with '2. Antivirus' highlighted), and 'Update Licenses' (listing various database expiry dates, with '4. Anti-Virus Database: Expiry Date: 2018-07-21' highlighted).

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

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

Navigation

Status

Network

Objects

Policies

System

General

System

Logging Options

Alarm Options

Administrator

Maintenance

Backup/Restore

Update

Database Update

Upgrade

Reboot

Database Update

Enable

Disable

Offline Update

Update Now

Update Server

Proxy Options

Refresh

Status: Not updating

No.	Database	Current Version	Latest Version	Update Svc Expira...	Auto Update	Operation
1	Anti-Virus Database	2017-12-29 Logs	2017-12-29	2018-07-21	✓	
2	URL Database	2017-12-25 Logs	2017-12-25	2018-07-21	✓	
3	Exploit Protection Database	2017-12-22 Logs	2017-12-22	2018-07-21	✓	
4	Software Update	af740_kb002_sp af740_kb001_sp	af740_kb002_sp af740_kb001_sp	Never expire	✓	
5	Application Ident Database	2017-12-11 Logs	2017-12-11	2018-07-21	✓	
6	WAF Signature Database	2017-12-20 Logs	2017-12-20	2018-07-21	✓	
7	Data Leak Protection	2017-12-29 Logs	2017-12-29	2018-07-21	✓	
8	Malware Signature Database	2017-12-28 Logs	2017-12-28	2018-07-21	✓	
9	Vulnerability Analysis Rule	2017-12-27 Logs	2017-12-27	2018-07-21	✓	
10	Malicious Connection Database	2017-12-13 Logs	2017-12-13	Never expire	✓	
11	Threat Intelligence Database	2017-12-04 Logs	2017-12-04	Never expire	✓	

5.2 Configuration of Anti-Virus

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

Navigation<<

Status

Network

Objects

Network Objects

Services

Security Policy Template

Exploit Protection

Web App Protection

APT Detection

Content Security

Threat Signature Databases

Content Control Databases

Content SecurityPolicies✕

+ Add✕ Delete🔄 Refresh

<input type="checkbox"/>	No.	Name
<input checked="" type="checkbox"/>	1	AntiVirus
<input type="checkbox"/>	2	Default Template

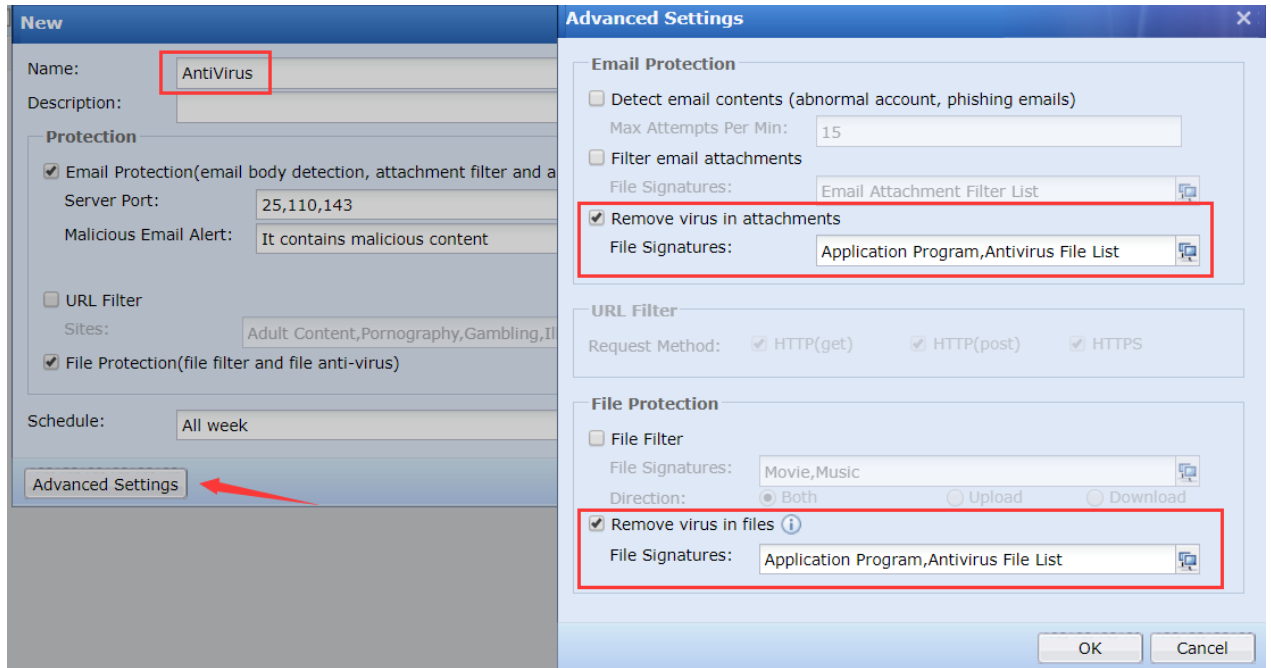
5.2.2 From New Template insert a name for the policy. The protection tick on the Email Protection and File Protection. The server port and malicious email alert leave it as default. After that click on the Advance Settings then tick on the Remove virus in attachments and Remove virus in files only. The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

Your Future-Proof IT Enabler

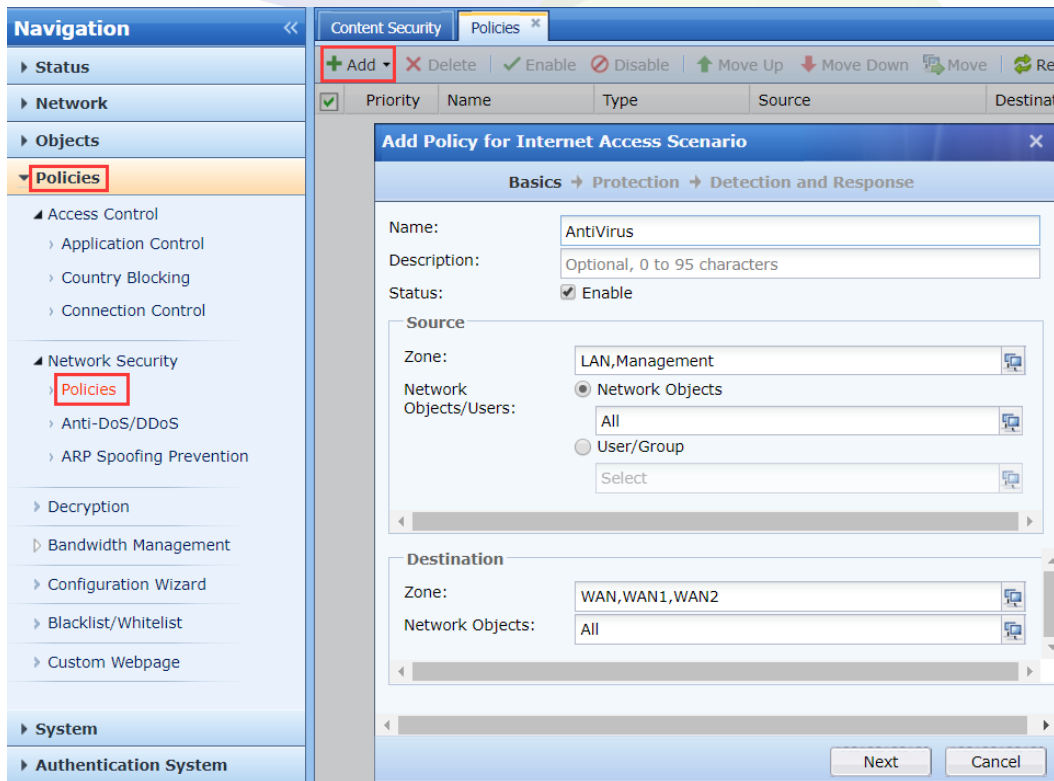
Sangfor Technologies

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



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.



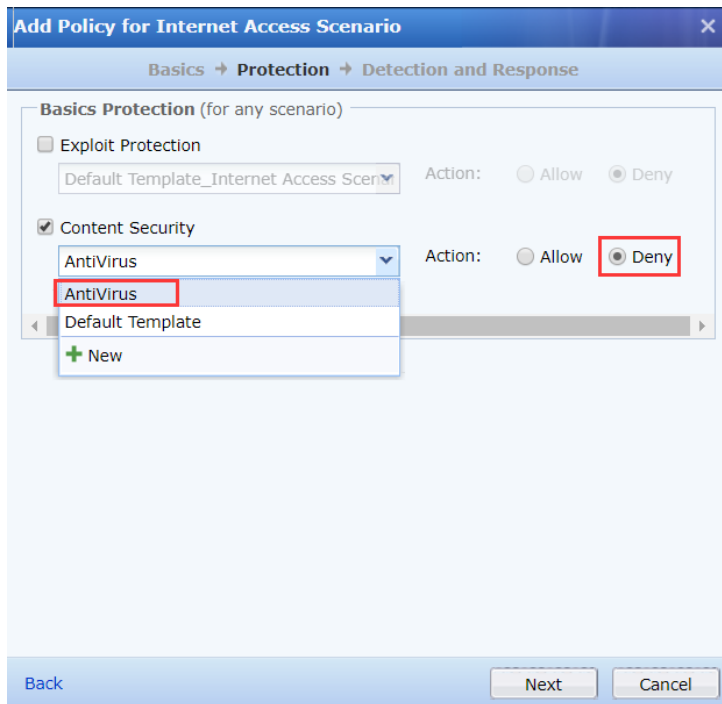
Your Future-Proof IT Enabler

Sangfor Technologies

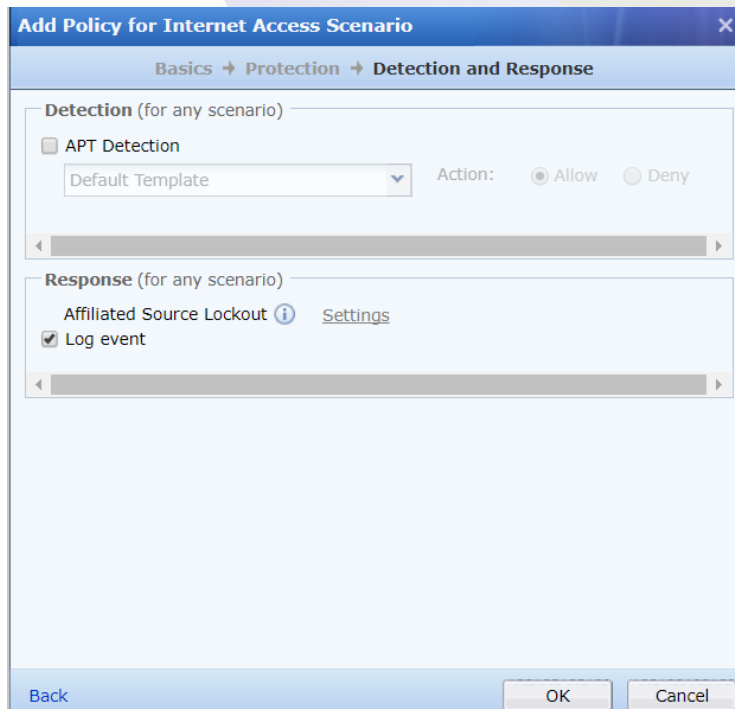
Block A1, Nanshan iPark, No.1001 Xueyuan Road, Nanshan District, Shenzhen, China

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

- 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.



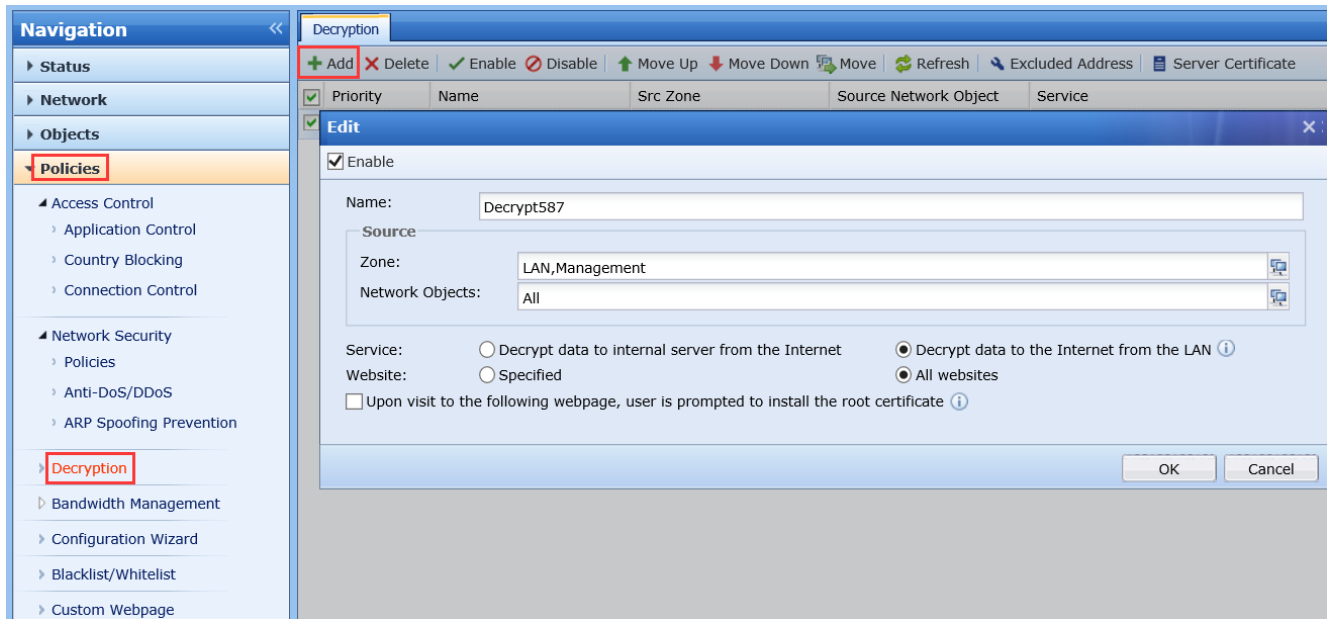
Your Future-Proof IT Enabler

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

- 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.

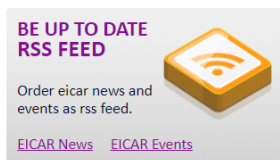


6 Anti-Virus function testing

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.



infected file. Read the user's manual of your AV scanner what to do or contact the vendor/manufacturer of your AV scanner.

IMPORTANT NOTE

EICAR cannot be held responsible when these files or your AV scanner in combination with these files cause any damage to your computer. **YOU DOWNLOAD THESE FILES AT YOUR OWN RISK.** Download these files only if you are sufficiently secure in the usage of your AV scanner. EICAR cannot and will not provide any help to remove these files from your computer. Please contact the manufacturer/vendor of your AV scanner to seek such help.

Download area using the standard protocol http

eicar.com 68 Bytes	eicar.com.txt 68 Bytes	eicar_com.zip 184 Bytes	eicarcom2.zip 308 Bytes
---------------------------------------	---	--	--

Download area using the secure, SSL enabled protocol https

eicar.com 68 Bytes	eicar.com.txt 68 Bytes	eicar_com.zip 184 Bytes	eicarcom2.zip 308 Bytes
---------------------------------------	---	--	--

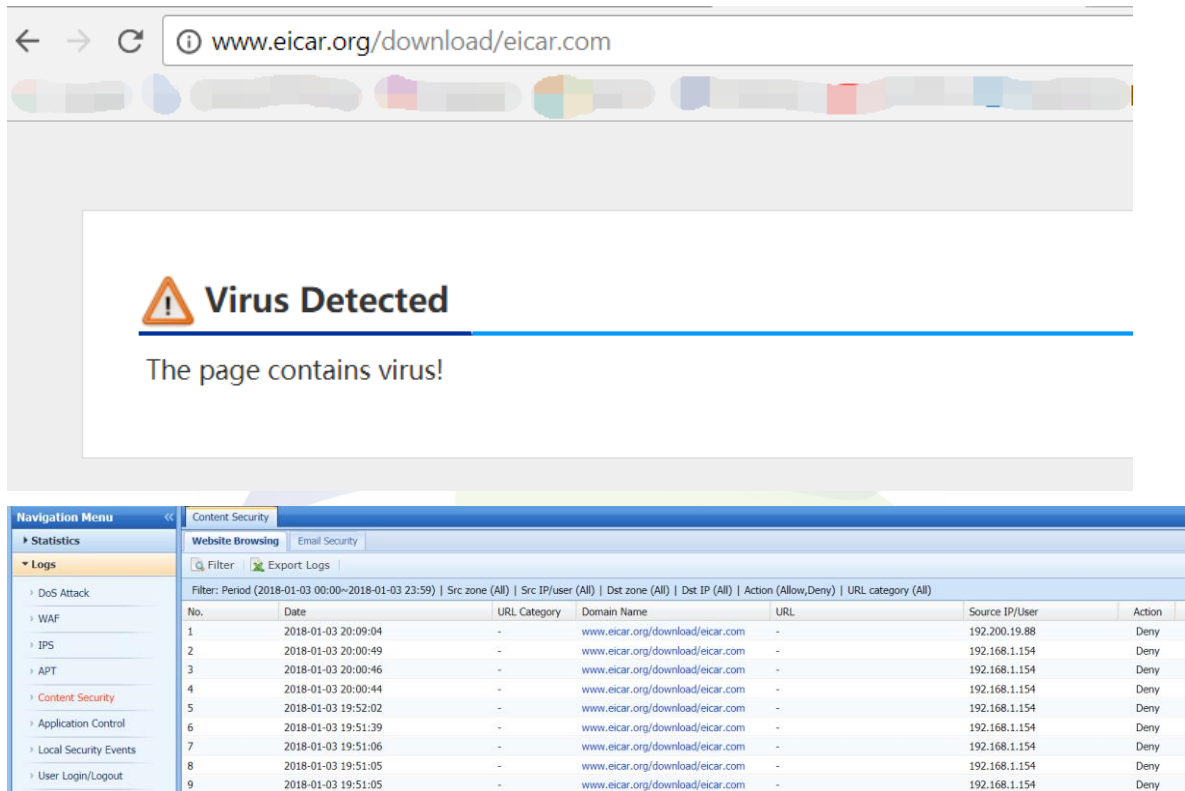
Your Future-Proof IT Enabler

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

- 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]



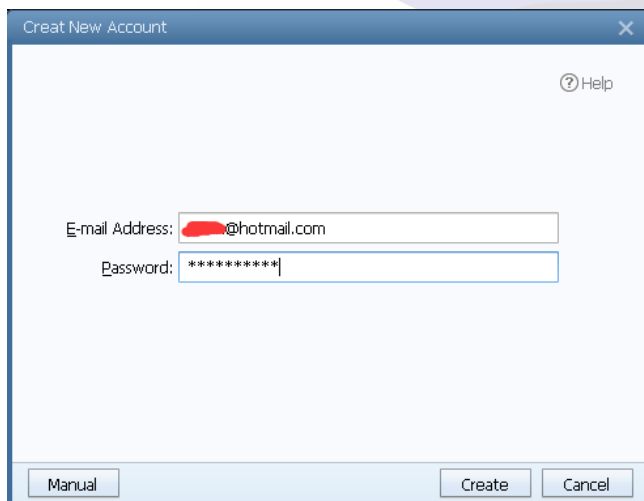
The first screenshot shows a web browser at www.eicar.org/download/eicar.com displaying a "Virus Detected" warning: "The page contains virus!".

The second screenshot shows the Sangfor management console. The left sidebar has a "Navigation Menu" with "Logs" expanded. The main area shows "Website Browsing" logs under "Content Security". The logs table is as follows:

No.	Date	URL Category	Domain Name	URL	Source IP/User	Action
1	2018-01-03 20:09:04	-	www.eicar.org/download/eicar.com	-	192.200.19.88	Deny
2	2018-01-03 20:00:49	-	www.eicar.org/download/eicar.com	-	192.168.1.154	Deny
3	2018-01-03 20:00:46	-	www.eicar.org/download/eicar.com	-	192.168.1.154	Deny
4	2018-01-03 20:00:44	-	www.eicar.org/download/eicar.com	-	192.168.1.154	Deny
5	2018-01-03 19:52:02	-	www.eicar.org/download/eicar.com	-	192.168.1.154	Deny
6	2018-01-03 19:51:39	-	www.eicar.org/download/eicar.com	-	192.168.1.154	Deny
7	2018-01-03 19:51:06	-	www.eicar.org/download/eicar.com	-	192.168.1.154	Deny
8	2018-01-03 19:51:05	-	www.eicar.org/download/eicar.com	-	192.168.1.154	Deny
9	2018-01-03 19:51:05	-	www.eicar.org/download/eicar.com	-	192.168.1.154	Deny

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.



The "Creat New Account" dialog box shows the following fields and buttons:

- E-mail Address:** [redacted]@hotmail.com
- Password:** [masked with asterisks]
- Buttons:** Manual, Create, Cancel
- Help:** A question mark icon with the text "Help".

Your Future-Proof IT Enabler

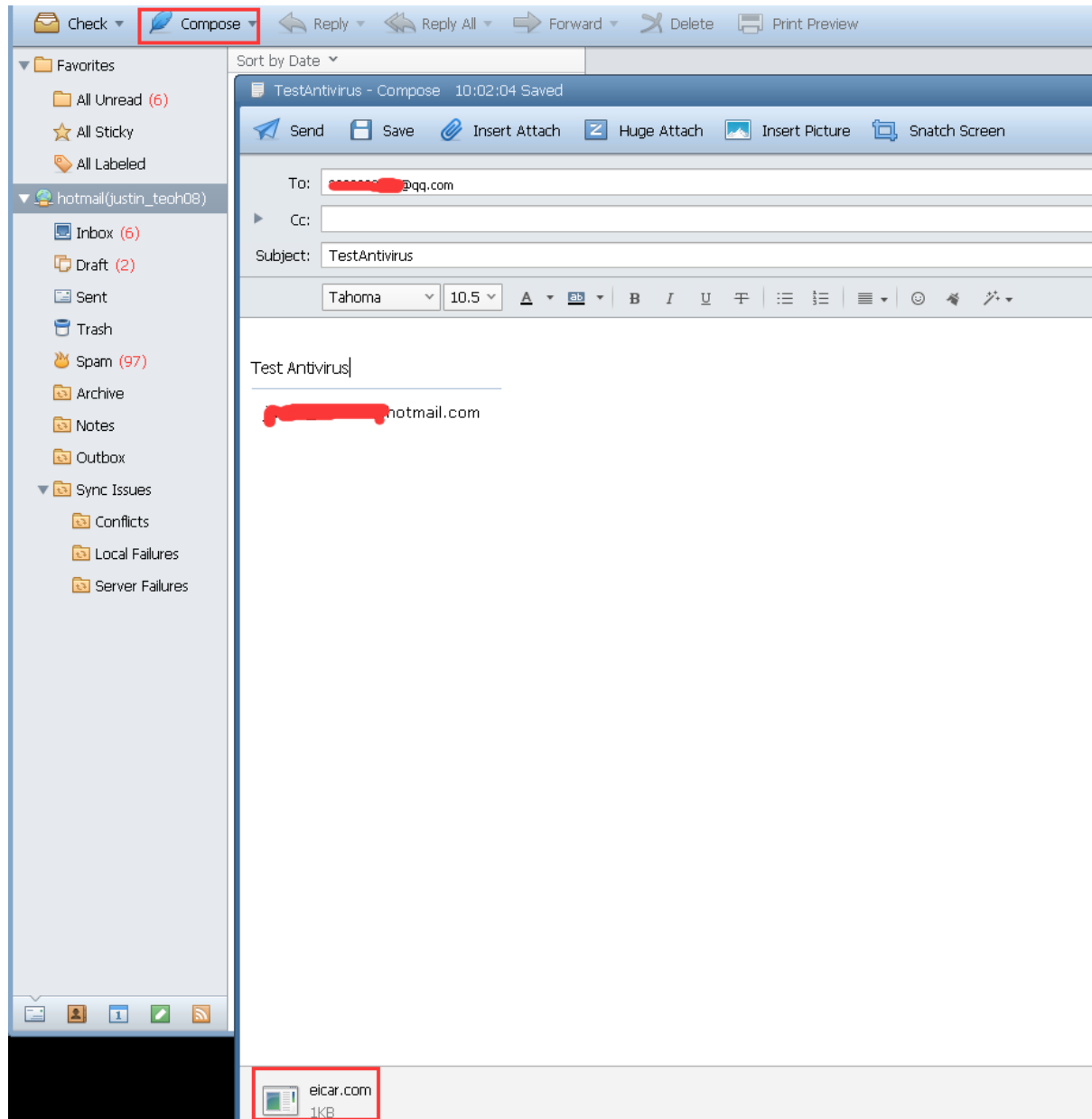
Sangfor Technologies

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

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.



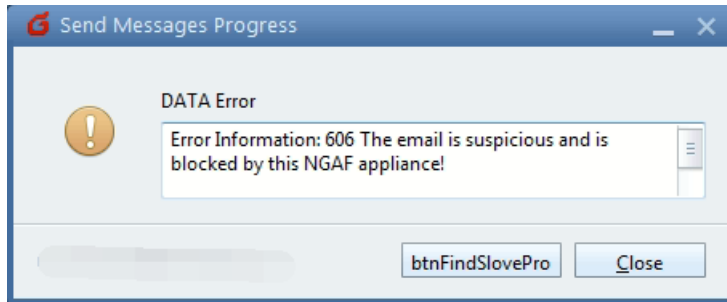
6.2.3 Foxmail shows error message: 606 The email is suspicious and is blocked by this NGAF appliance!

Your Future-Proof IT Enabler

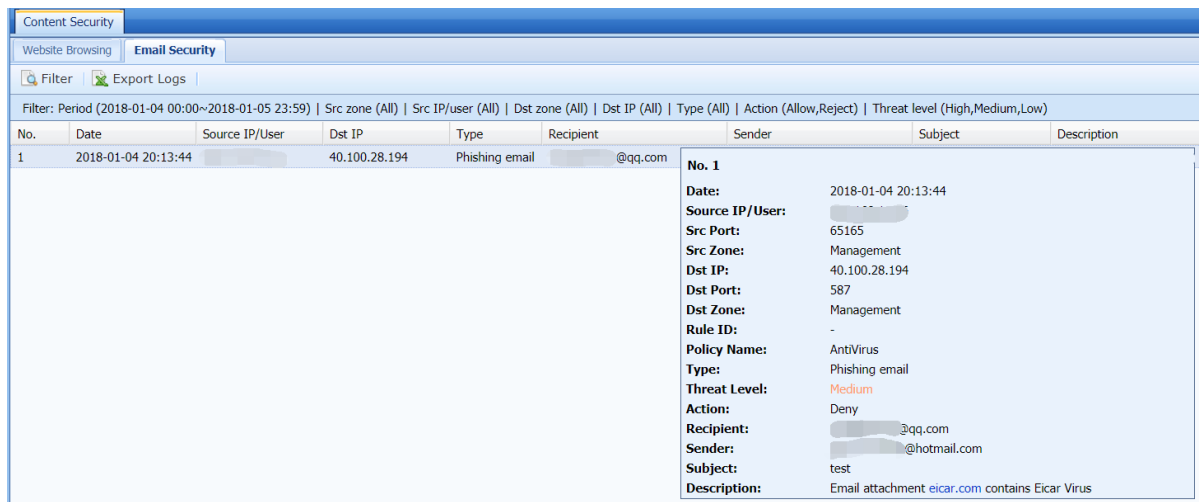
Sangfor Technologies

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



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



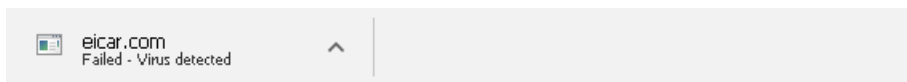
7 Attentions

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.

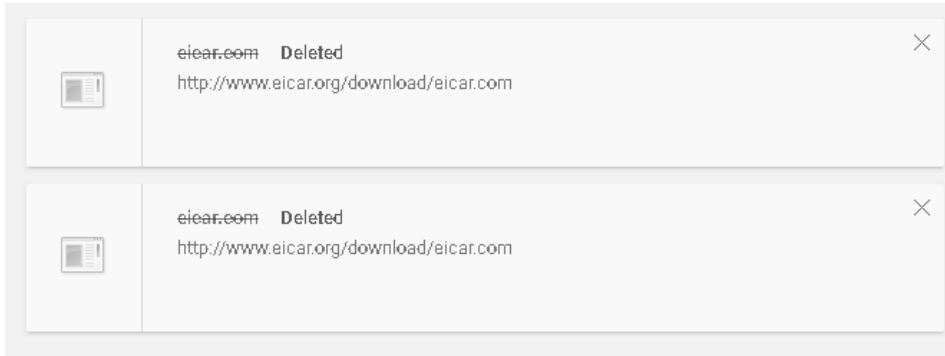


Your Future-Proof IT Enabler

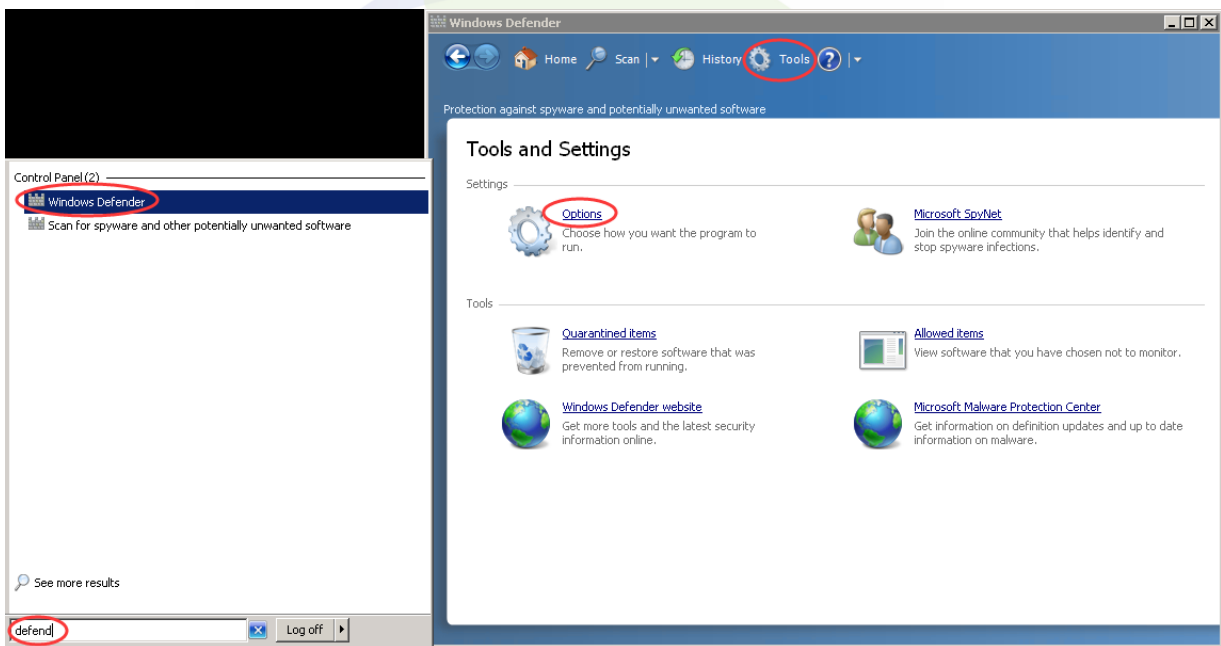
Sangfor Technologies

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



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.

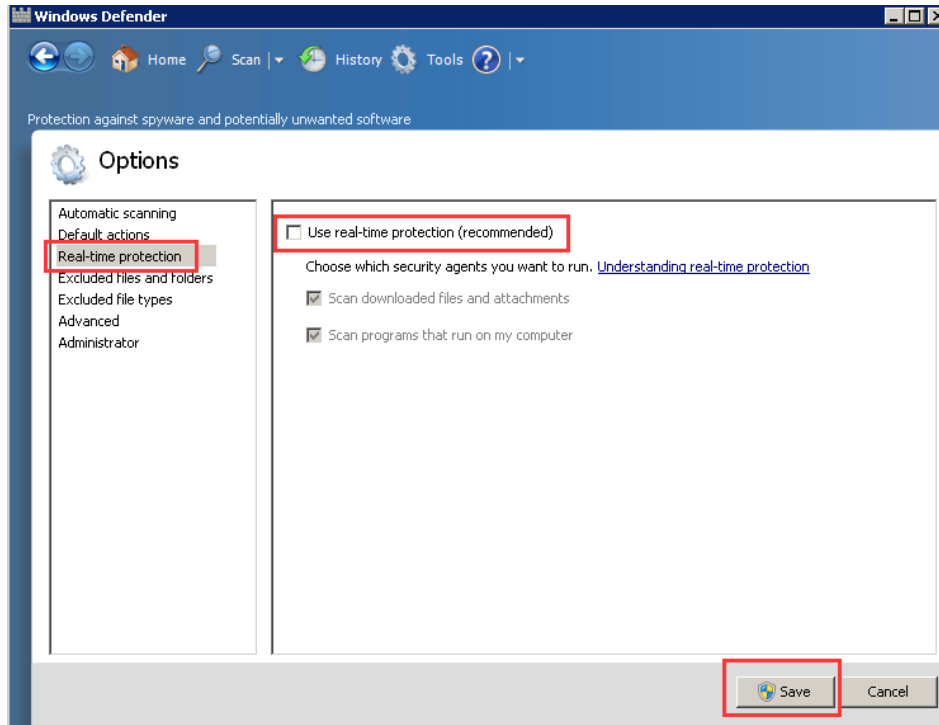


Your Future-Proof IT Enabler

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



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)

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