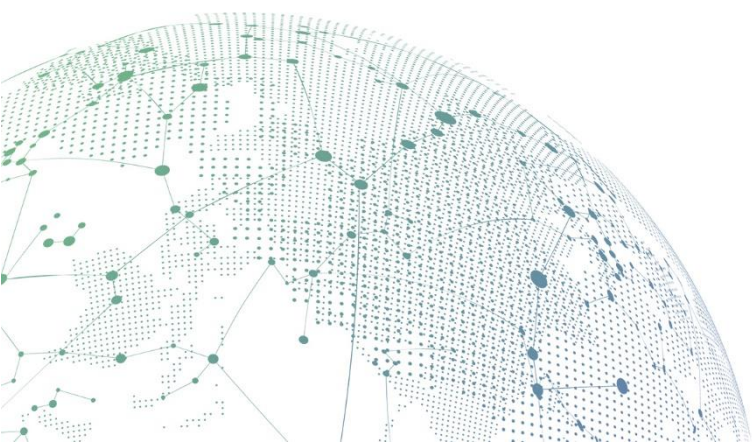




IAM

Neural-X Anti-Virus Configuration Guide

Version 12.0.18



Change Log

Date	Change Description
Dec 24, 2019	Version 12.0.18 document release.

CONTENT

Chapter 1 Content requirements	1
1 Product Introduction	1
2 Application Scenario	1
3 Testing environment	1
3.1 Topology	1
3.2 Testing requirement.....	1
4 Configuration Guide with Screenshot	2
4.1 SMTP anti-virus	2
5 Conclusion	7

Chapter 1 Content requirements

1 Product Introduction

The main function of the Neural-X is to protect the internal user from virus and other network attack. Besides, it able to improve the security of internal network environment. The virus that infect user usually from these path, HTTP, FTP, SMTP, document transfer and etc. Neural-X is mainly focus on these type of transfer method to perform anti-virus.

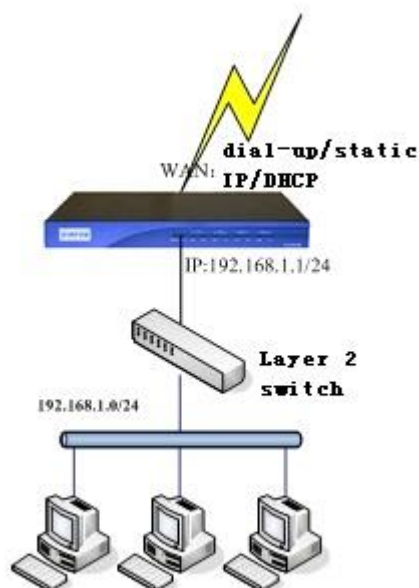
2 Application Scenario

Neural-X is mainly focus on these type of transfer method to perform anti-virus.

1. FTP
2. HTTP
3. SMTP
4. POP3

3 Testing environment

3.1 Topology



IAM device in route or bridge deployment mode.

3.2 Testing requirement

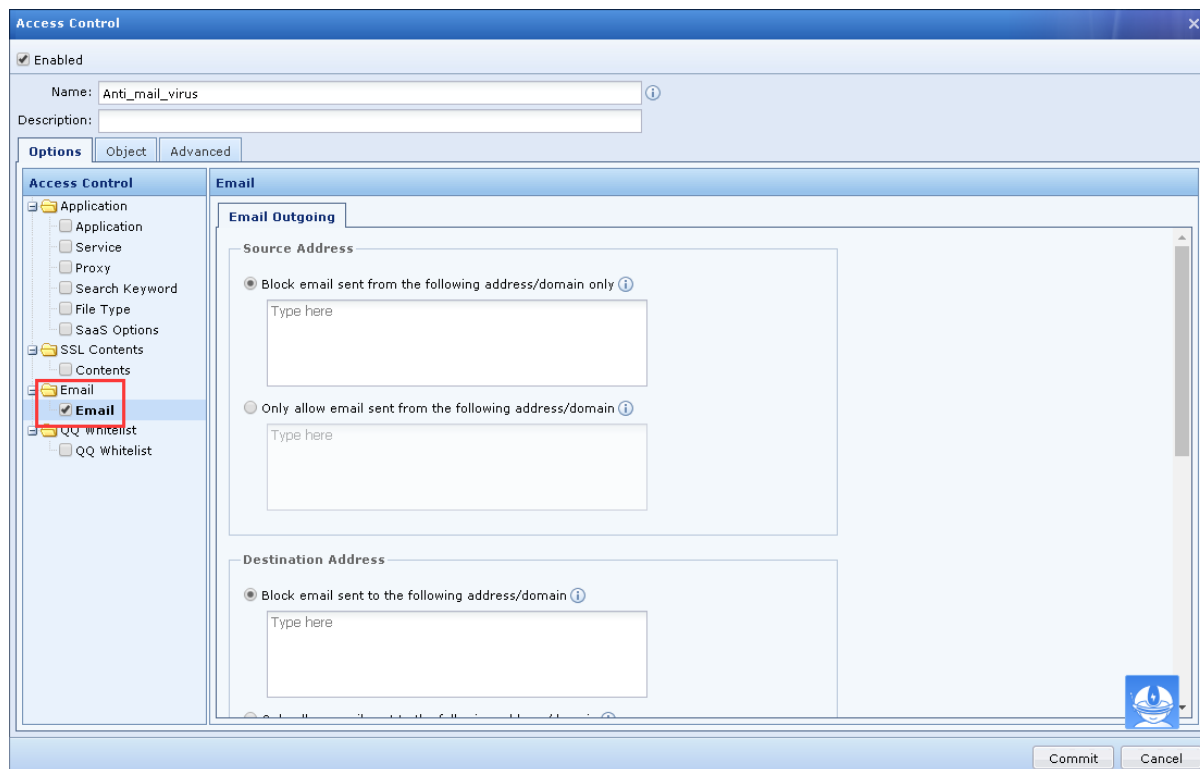
1. IAM device with the valid Neural-X license.
2. Ensure the traffic is passing through IAM.
3. The anti-virus for SMTP/POP3 protocol is implemented by device proxy, ensure the communication between IAM and Mail server/Mail client is normal.

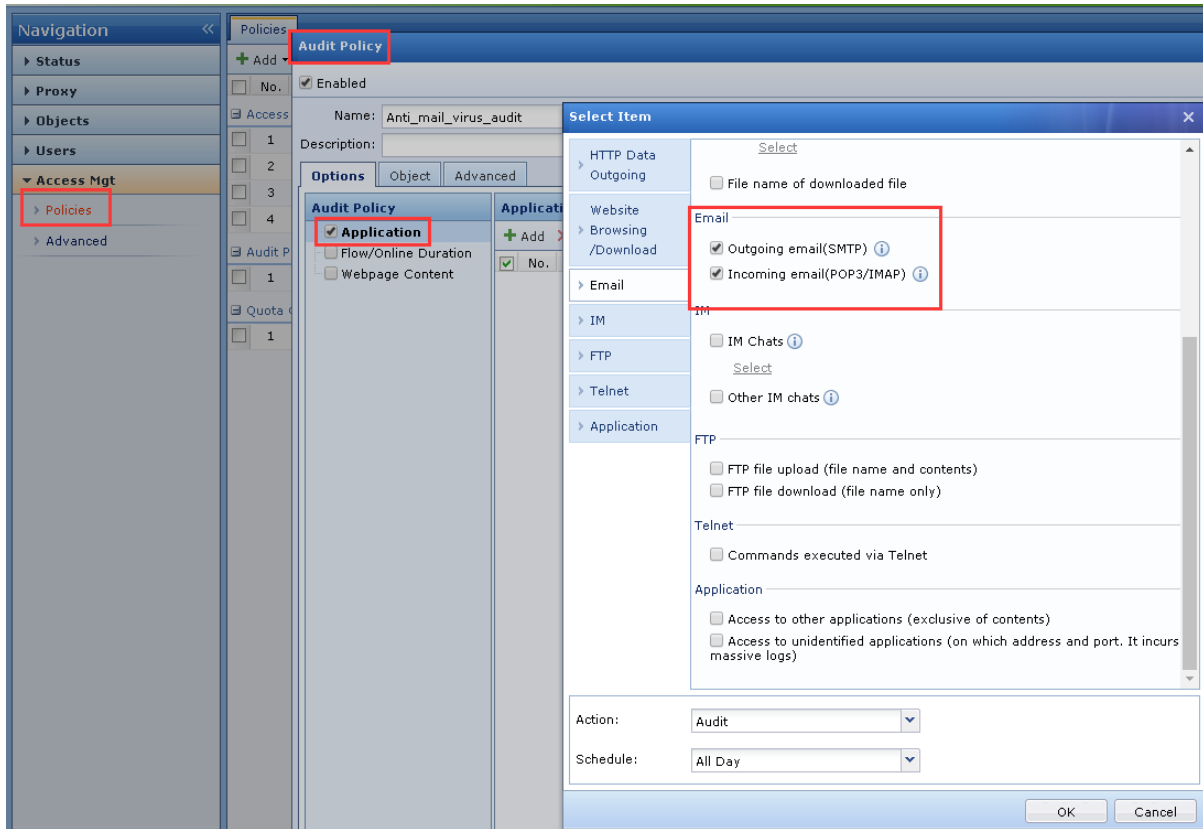
4 Configuration Guide with Screenshot

4.1 SMTP anti-virus

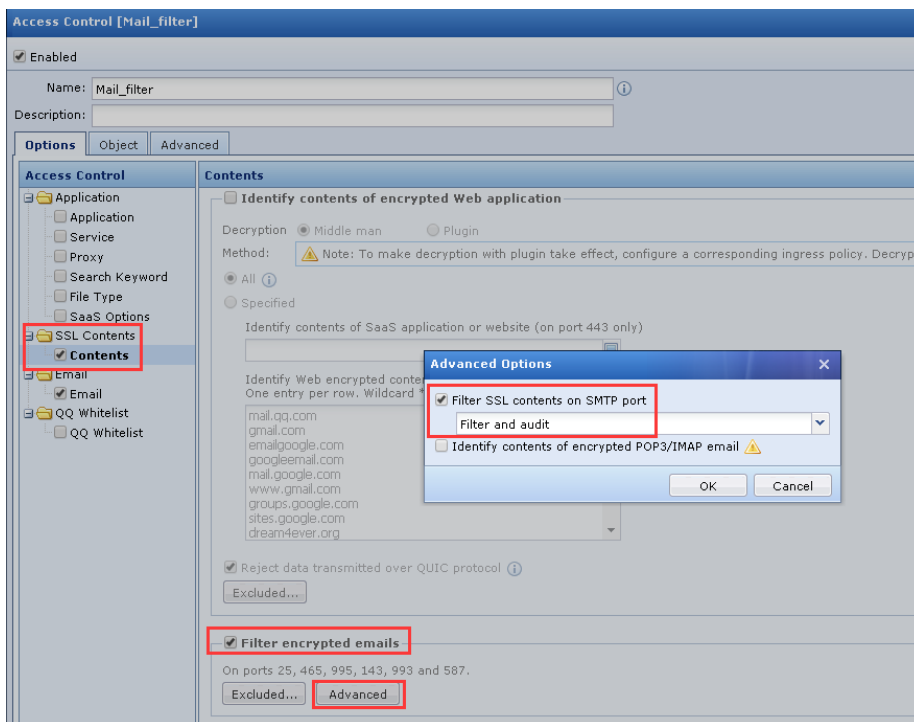
As below will be the SMTP anti-virus progress.

1. Configure an **Access Control policy** with enable the “**Email**” filter function as well as configure a **Audit policy** to audit the email, assign to the specific user.

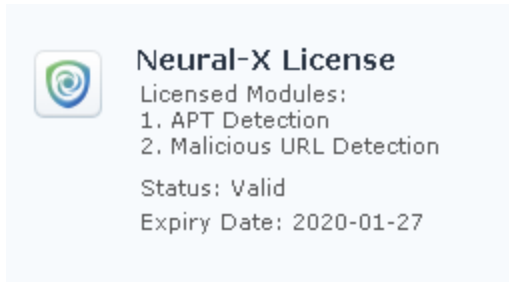




2. If the email client has configure with a secure SMTP/POP3, we need to enable the [SSL content] function on the Mail_filter policy. Enable the [SSL content] function is able to encrypt the email and identify the source mail domain.

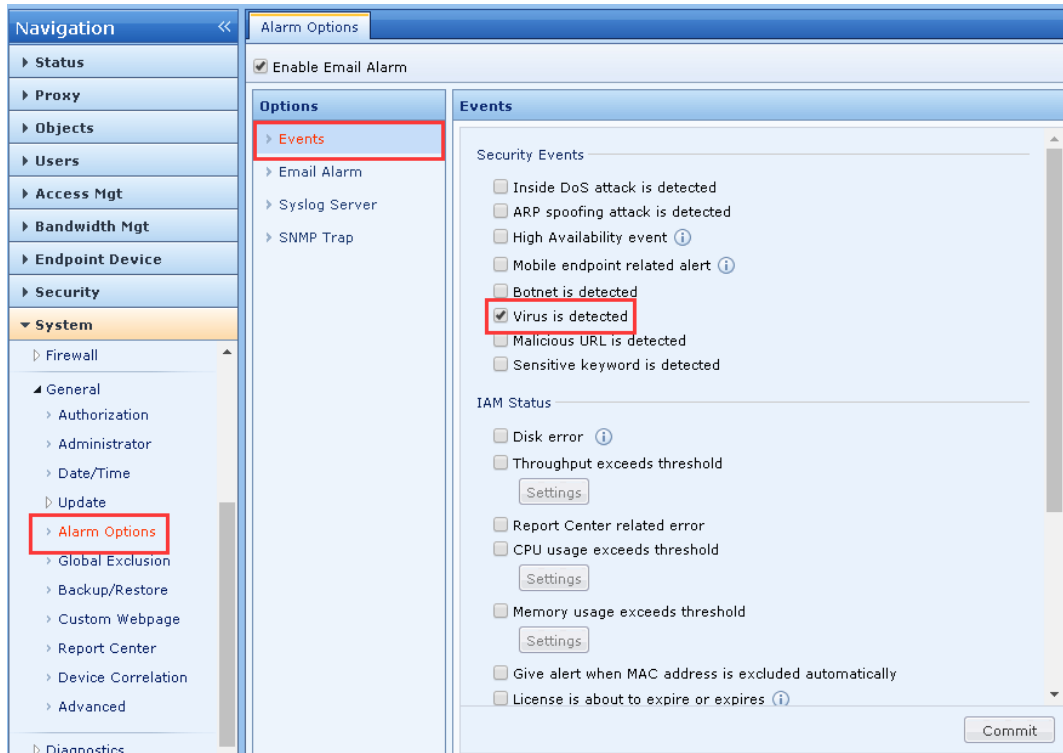


3. 2. Ensure the Neural-X is functionable with a available license key.



Neural-X License
Licensed Modules:
1. APT Detection
2. Malicious URL Detection
Status: Valid
Expiry Date: 2020-01-27

- 4. Enable the alarm option at [System] – [Alarm option] to inform the related admin when the virus is detected. The configuration as diagram below.



The screenshot shows the 'Alarm Options' configuration page. On the left is a navigation tree with 'System' expanded and 'Alarm Options' selected. The main area is titled 'Alarm Options' and has a checked 'Enable Email Alarm' option. Under 'Options', 'Events' is selected. The 'Events' section lists several security events, with 'Virus is detected' checked. Other events include 'Inside DoS attack is detected', 'ARP spoofing attack is detected', 'High Availability event', 'Mobile endpoint related alert', 'Botnet is detected', 'Malicious URL is detected', and 'Sensitive keyword is detected'. Below this is the 'IAM Status' section with options for 'Disk error', 'Throughput exceeds threshold', 'Report Center related error', 'CPU usage exceeds threshold', 'Memory usage exceeds threshold', 'Give alert when MAC address is excluded automatically', and 'License is about to expire or expires'. A 'Commit' button is at the bottom right.

Options

- > Events
- > Email Alarm**
- > Syslog Server
- > SNMP Trap

Email Alarm

Outgoing Mail Server

Sender Address: test@gmail.com

Server Address: smtp.gmail.com

Server Port: 465

Authentication required

Username: test@gmail.com

Password: ●●●

Email Delivery

Recipient: test1@gmail.com ⓘ

Subject: Alert Message from Sangfor Appliance

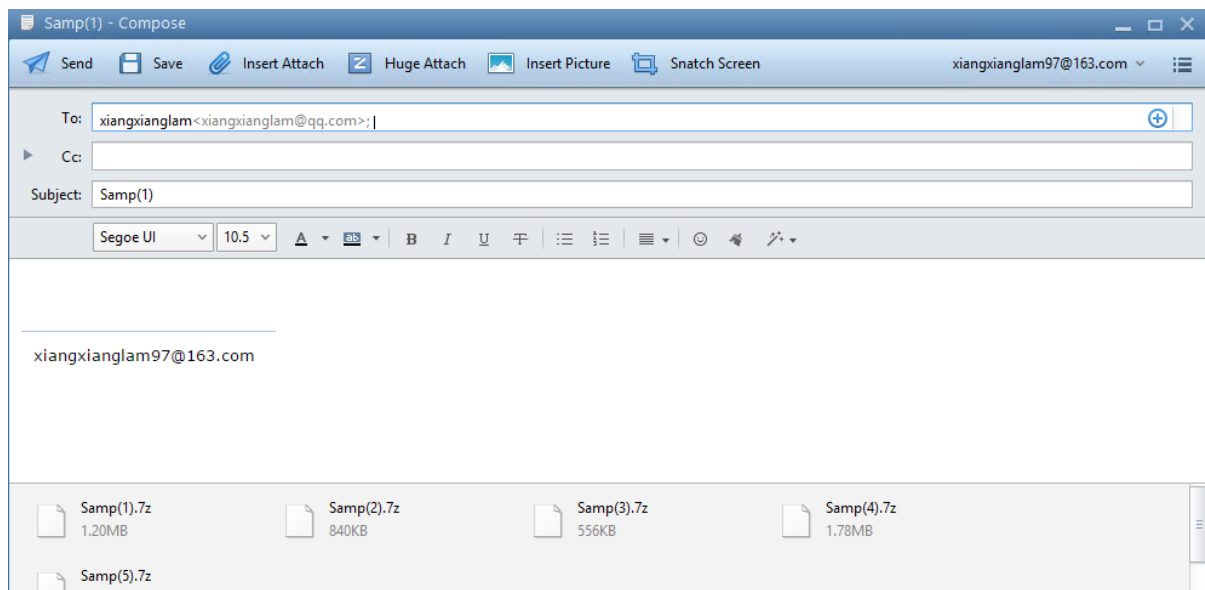
Interval: Sent immediately Every (minute) ⓘ

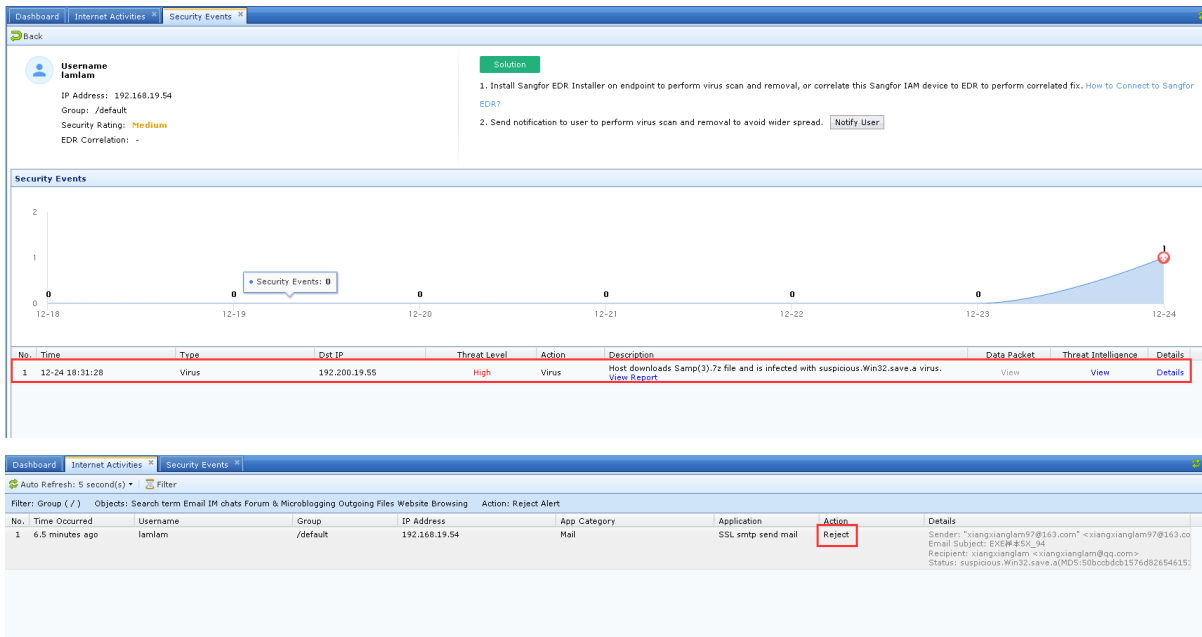
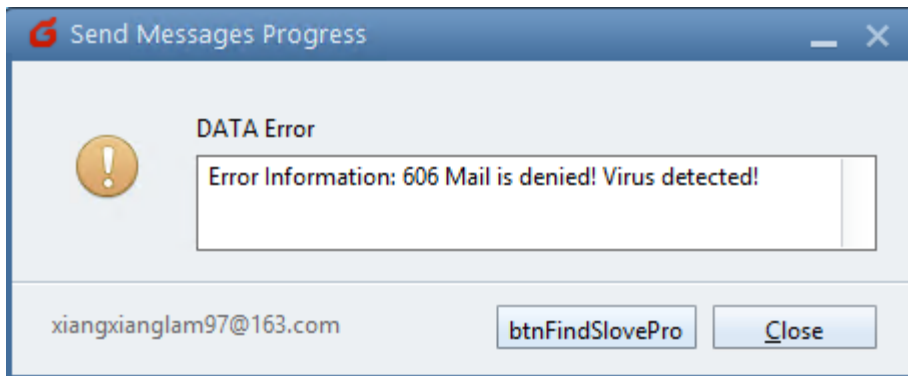
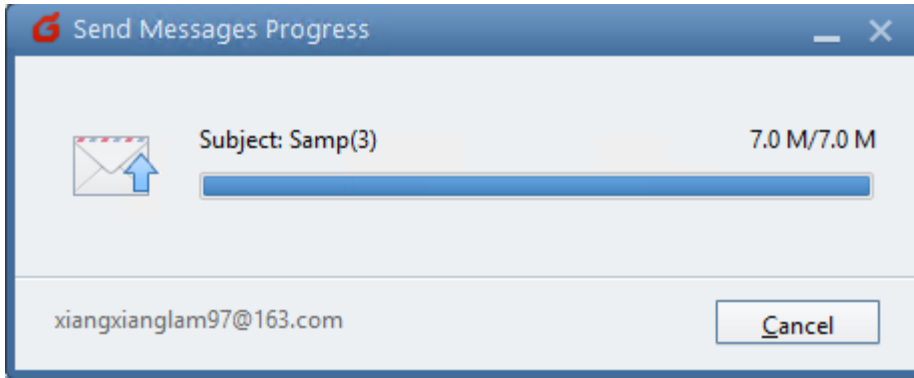
1

Send Testing Email Commit

After finished all the setting as diagram above, by using a pc with Foxmail (**mail client**), send a virus email for testing purpose.

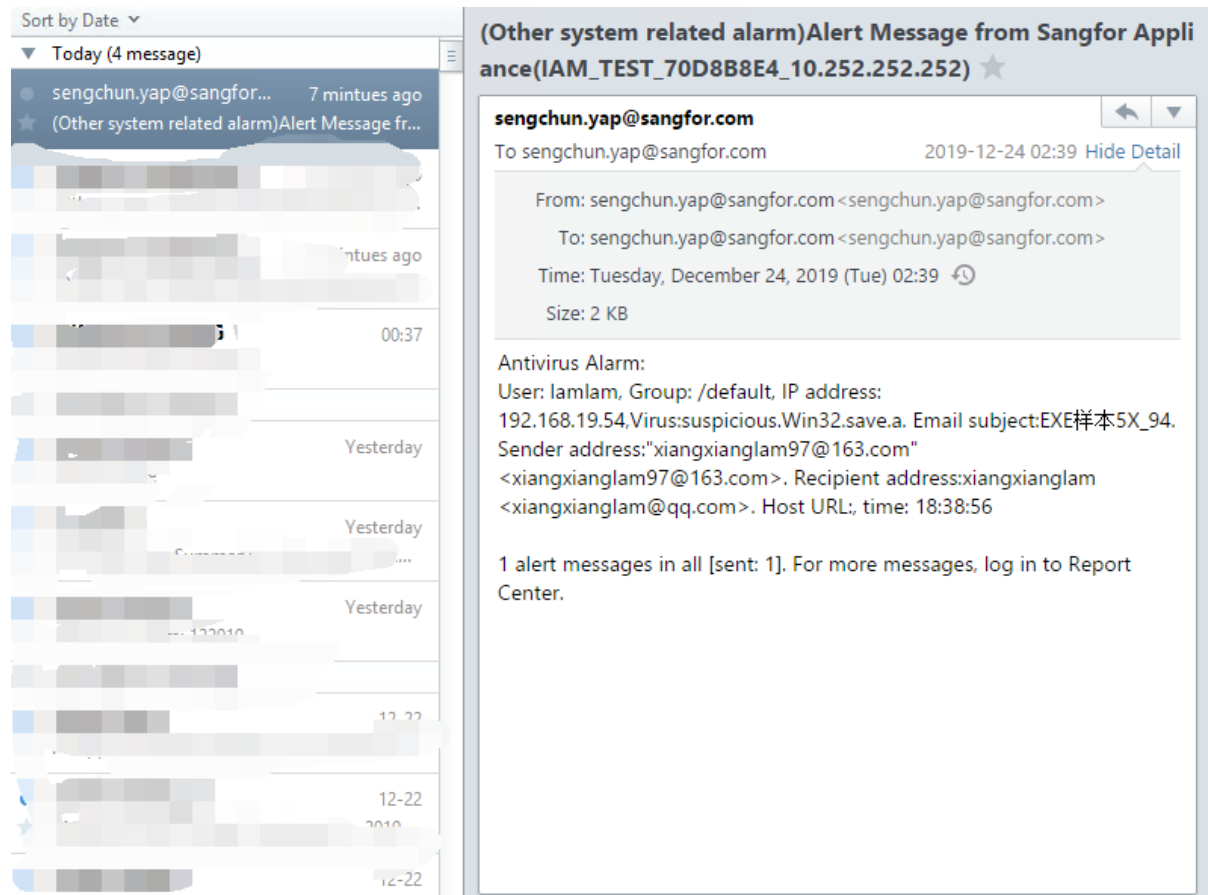
1. Send a virus email through Foxmail as diagram below:





As the diagram above show the email has been block due to the content with virus file detected.

2. Alert Message from IAM that virus has been detected.



5 Conclusion

The Neural-X module is able to detect and block the virus through FTP, HTTP, SMTP/POP3, else it able send virus alarm email to specific admin to effectively protect the security of intranet users.



SANGFOR

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 is the trademark 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