



SANGFOR

# **SANGFOR \_NGAF \_v7.4\_ Application Control and Web Filtering Configuration Guide**

SANGFOR Technologies Inc.

6<sup>th</sup> December 2017

*Your Future-Proof IT Enabler*

**Sangfor Technologies**

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


T.: +86 755 2189 0000 (7511) | E.: tech.support@sangfor.com | W.: www.sangfor.com



## Declaration

Copyright © SANGFOR Technologies Inc. All rights reserved.

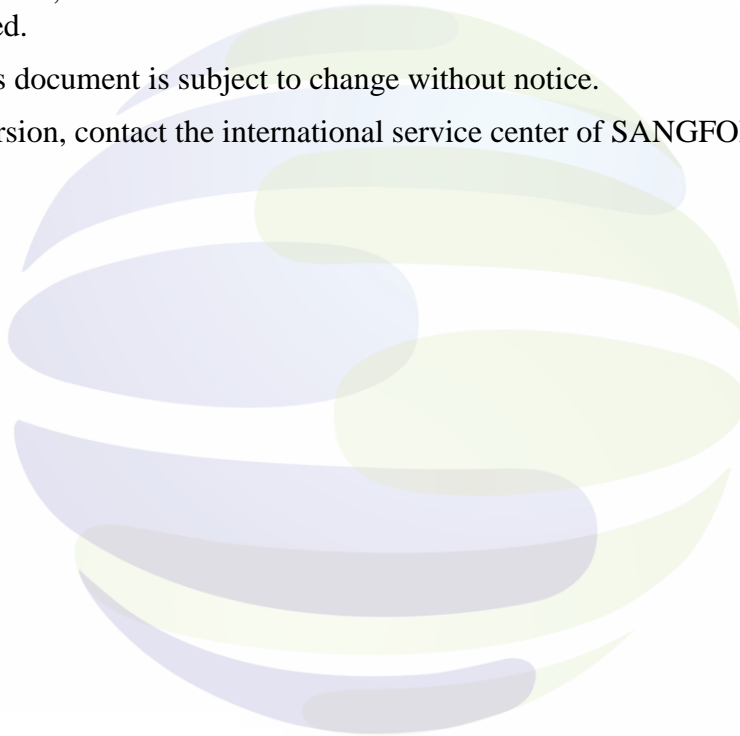
No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.

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

<b>Declaration</b>	2
Table of contents	3
<b>1 Introduction</b>	4
1.1 Abbreviations and conventions	4
1.2 Feedback	4
<b>2 Scenario</b>	4
2.1 Prerequisite	5
<b>3 Configuration Steps</b>	5
3.1 Basic setting	5
3.2 URL Filtering	6
3.3 Application control	8
<b>4 Test Results</b>	9
4.1 Unable to access online shopping website. ( <i>Example: taobao.com</i> )	9
4.2 Failed to watch online streaming media	9
<b>5 Precautions</b>	9

*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

NGAF in this article refers to the SANGFOR NGAF device.

## 1.2 Feedback

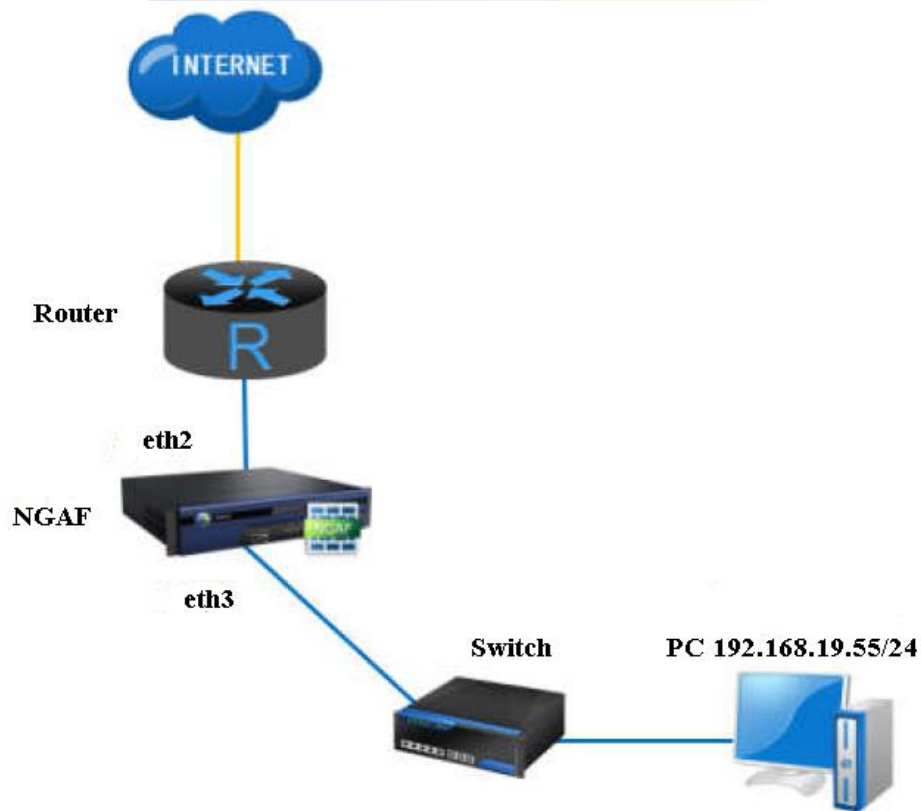
If you find any questions of this documents, please feel free to give us feedback, email: [tech.support@sangfor.com](mailto:tech.support@sangfor.com).

# 2 Scenario

To ensure company and department can operate normally and increase work efficiency, the application control policy and URL filtering should be configured in NGAF.

The purpose is to control LAN users use application and access website in working hours. This testing is to demonstrate how to block users watching online video and restrict users accessing shopping website.

Test environment is shown as below:



- WAN gateway: eth2.

*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](mailto:tech.support@sangfor.com) | W.: [www.sangfor.com](http://www.sangfor.com)



- LAN gateway: eth3.
- LAN PC: 192.168.19.55.
- Deployment: Bridge mode (access).

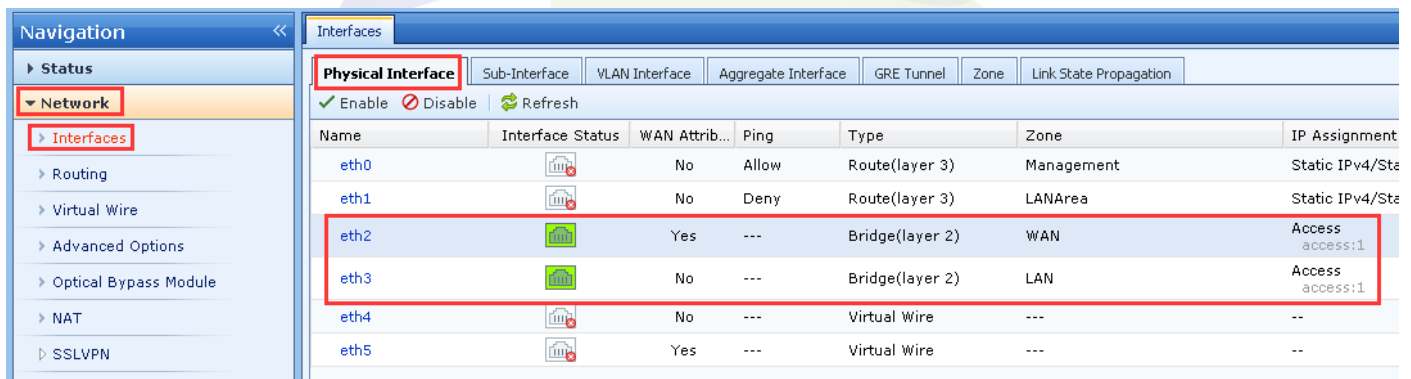
## 2.1 Prerequisite

- Make sure that Application Signature and URL Database upgrade to the latest version.
- The data flow of PC accessed to Internet must pass through NGAF.

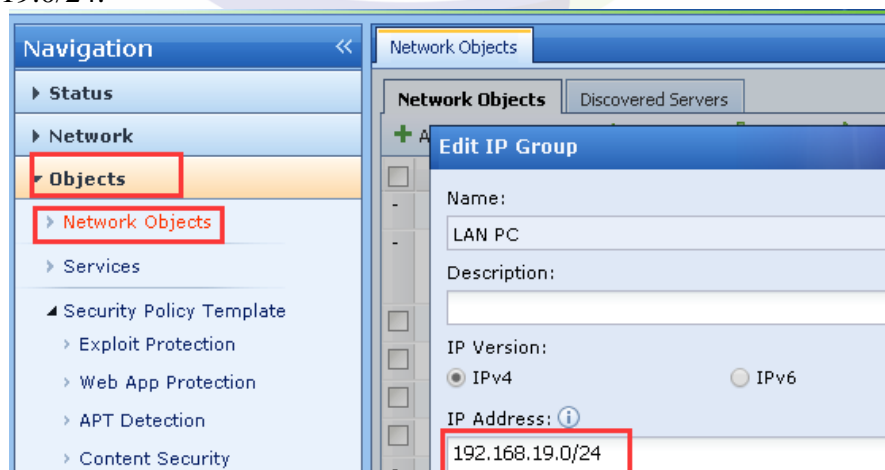
# 3 Configuration Steps

## 3.1 Basic setting

- Login to NGAF web console, configure the types of eth2 and eth3 as bridge mode and connection type is access with vlan1 in **Network>Interfaces>Physical Interface**. Besides, divide eth2 as WAN zone with select “WAN properties” and eth3 as LAN zone.



- In **Objects>Network Objects** to add “IP Group” for LAN zone PC with IP address 192.168.19.0/24.



Your Future-Proof IT Enabler

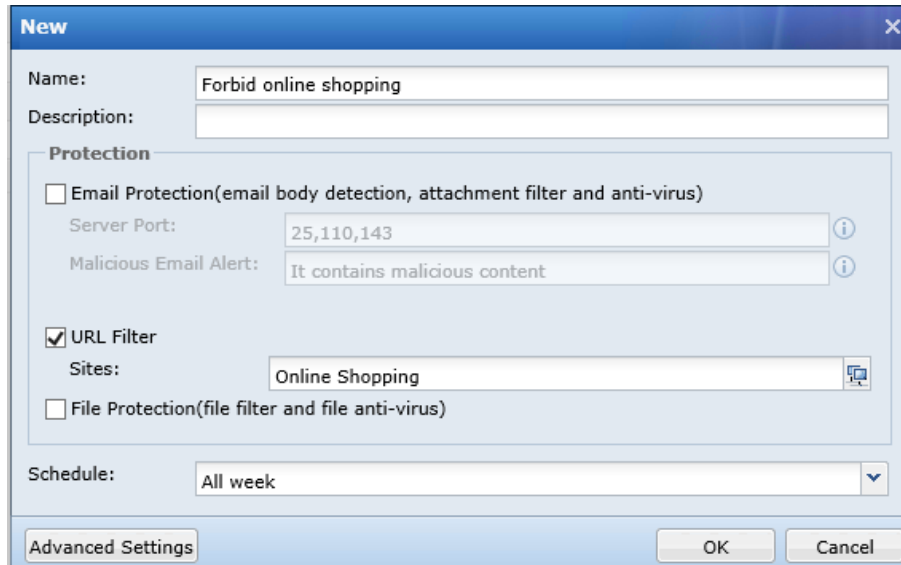
Sangfor Technologies

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

## 3.2 URL Filtering

- i. In **Objects > Security Policy Template > Content Security** to create a Content Security Template for “Forbid online shopping”.

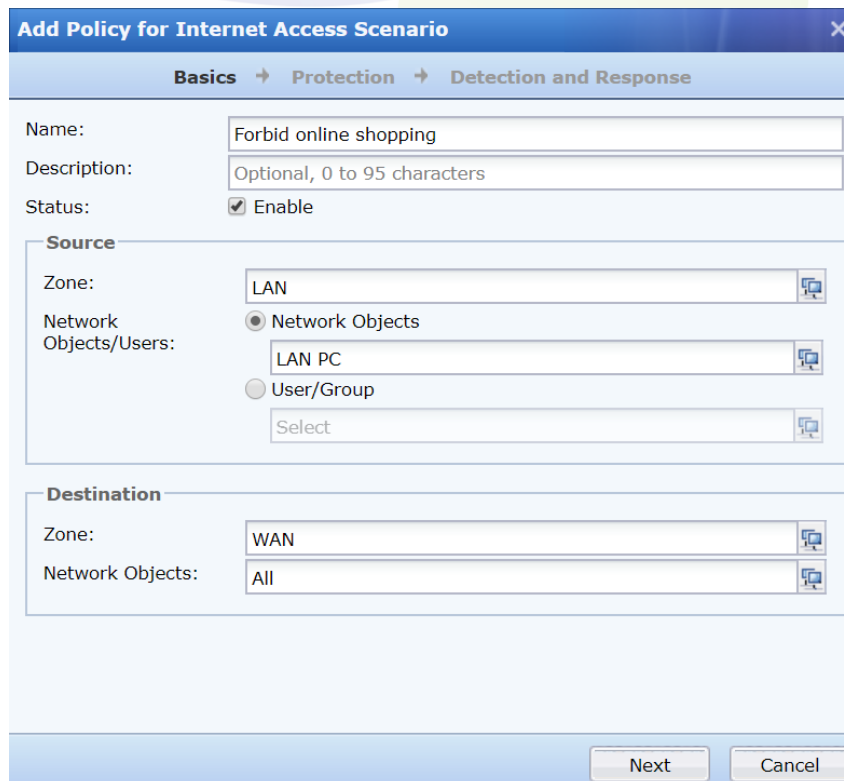


The 'New' dialog box is used to create a Content Security Template. It includes the following fields and options:

- Name:** Forbid online shopping
- Description:** (empty)
- Protection:**
  - ☐ Email Protection(email body detection, attachment filter and anti-virus)
    - Server Port:** 25,110,143
    - Malicious Email Alert:** It contains malicious content
  - ☒ URL Filter
    - Sites:** Online Shopping
  - ☐ File Protection(file filter and file anti-virus)
- Schedule:** All week

Buttons: Advanced Settings, OK, Cancel

- ii. In **Policies > Network Security > Policies** Create a Policy, click **add > Policy for Internet Access Scenario** to create a new policy for Forbid online shopping.



The 'Add Policy for Internet Access Scenario' dialog box is used to create a new policy. It includes the following fields and options:

- Name:** Forbid online shopping
- Description:** Optional, 0 to 95 characters
- Status:** ☒ Enable
- Source:**
  - Zone:** LAN
  - Network Objects/Users:**
    - ☒ Network Objects
      - LAN PC
    - ☐ User/Group
      - Select
- Destination:**
  - Zone:** WAN
  - Network Objects:** All

Buttons: Next, Cancel

*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



**Add Policy for Internet Access Scenario** ✕

Basics → Protection → Detection and Response

**Basics Protection** (for any scenario) ?

☐ Intrusion Prevention ?

Default Template\_Internet Access Scenario ▼

Action: ☐ Allow ☒ Deny

☒ Content Security ?

Forbid online shopping ▼

Action: ☐ Allow ☒ Deny

Back

Next

Cancel

**Add Policy for Internet Access Scenario** ✕

Basics → Protection → Detection and Response

**Detection** (for any scenario) ?

☐ APT Detection ?

Default Template ▼

Action: ☒ Allow ☐ Deny

**Response** (for any scenario) ?

Affiliated Source Lockout ? [Settings](#)

☒ Log event

Back

OK

Cancel

*Your Future-Proof IT Enabler*

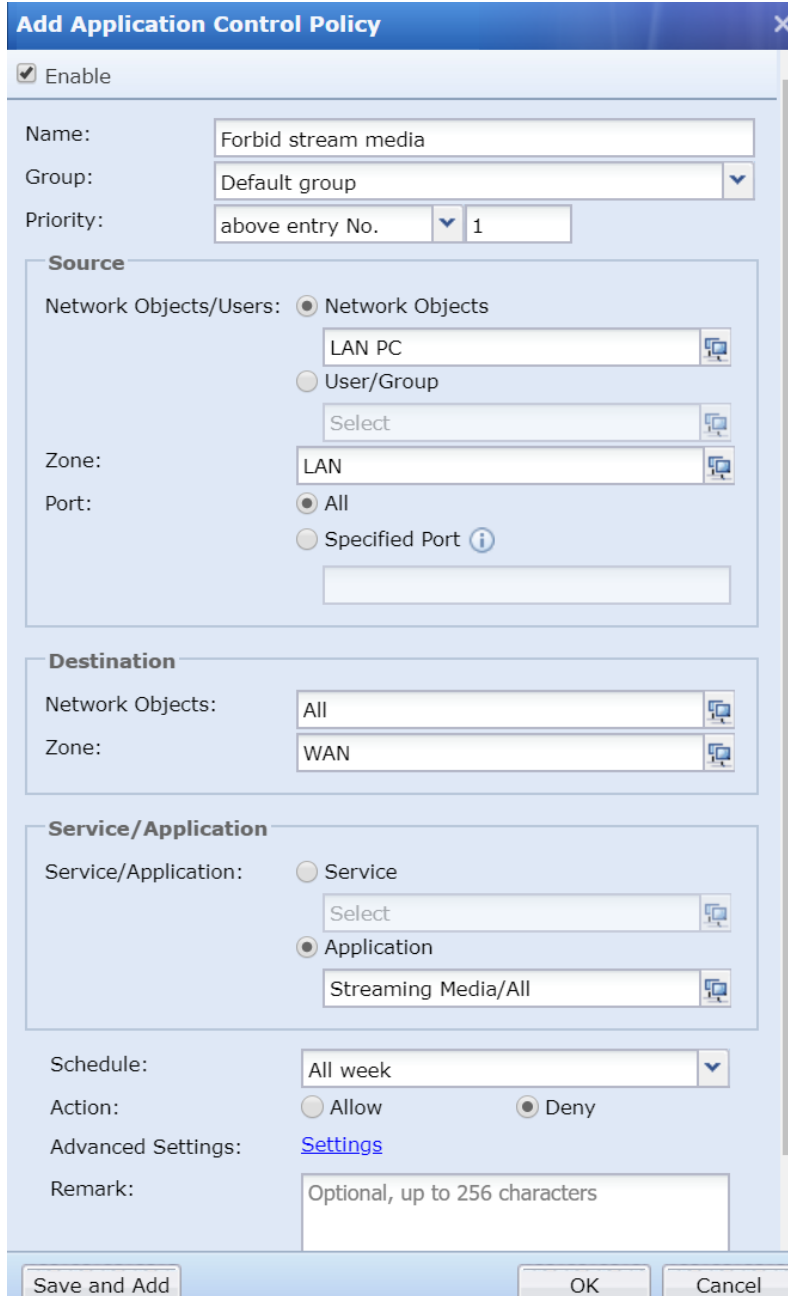
**Sangfor Technologies**

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

### 3.3 Application control

- i. In **Policies>Access Control>Application Control** to create a new policy “Forbid using application” to restrict users.
- Network Object: Target IP Group (Example: LAN PC)
  - Zone: LAN
  - Application: Select all the application which are related with QQ.



The screenshot shows the 'Add Application Control Policy' dialog box. It has a title bar with a close button. The 'Enable' checkbox is checked. The 'Name' field contains 'Forbid stream media'. The 'Group' dropdown is set to 'Default group'. The 'Priority' dropdown is set to 'above entry No.' with a value of '1'. The 'Source' section has 'Network Objects/Users' set to 'Network Objects' with 'LAN PC' selected. The 'Zone' is set to 'LAN'. The 'Port' is set to 'All'. The 'Destination' section has 'Network Objects' set to 'All' and 'Zone' set to 'WAN'. The 'Service/Application' section has 'Service/Application' set to 'Application' with 'Streaming Media/All' selected. The 'Schedule' dropdown is set to 'All week'. The 'Action' has 'Allow' and 'Deny' radio buttons, with 'Deny' selected. There is a 'Settings' link for 'Advanced Settings'. The 'Remark' field contains 'Optional, up to 256 characters'. At the bottom are 'Save and Add', 'OK', and 'Cancel' buttons.

**Add Application Control Policy**

☒ Enable

Name: Forbid stream media

Group: Default group

Priority: above entry No. 1

**Source**

Network Objects/Users: ☒ Network Objects  
LAN PC

☐ User/Group  
Select

Zone: LAN

Port: ☒ All  
☐ Specified Port

**Destination**

Network Objects: All

Zone: WAN

**Service/Application**

Service/Application: ☐ Service  
Select

☒ Application  
Streaming Media/All

Schedule: All week

Action: ☐ Allow ☒ Deny

Advanced Settings: [Settings](#)

Remark: Optional, up to 256 characters

Save and Add OK Cancel

*Your Future-Proof IT Enabler*

**Sangfor Technologies**

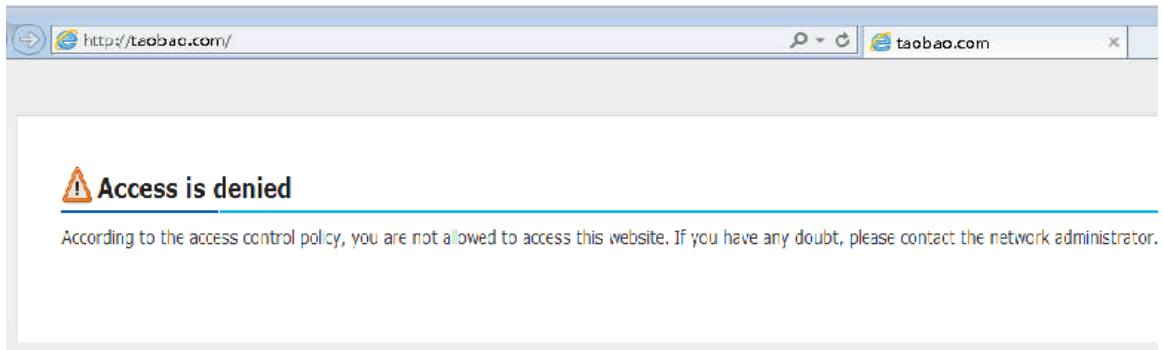
Block A1, Nanshan iPark, No.1001 Xueyuan Road, Nanshan District, Shenzhen, China

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

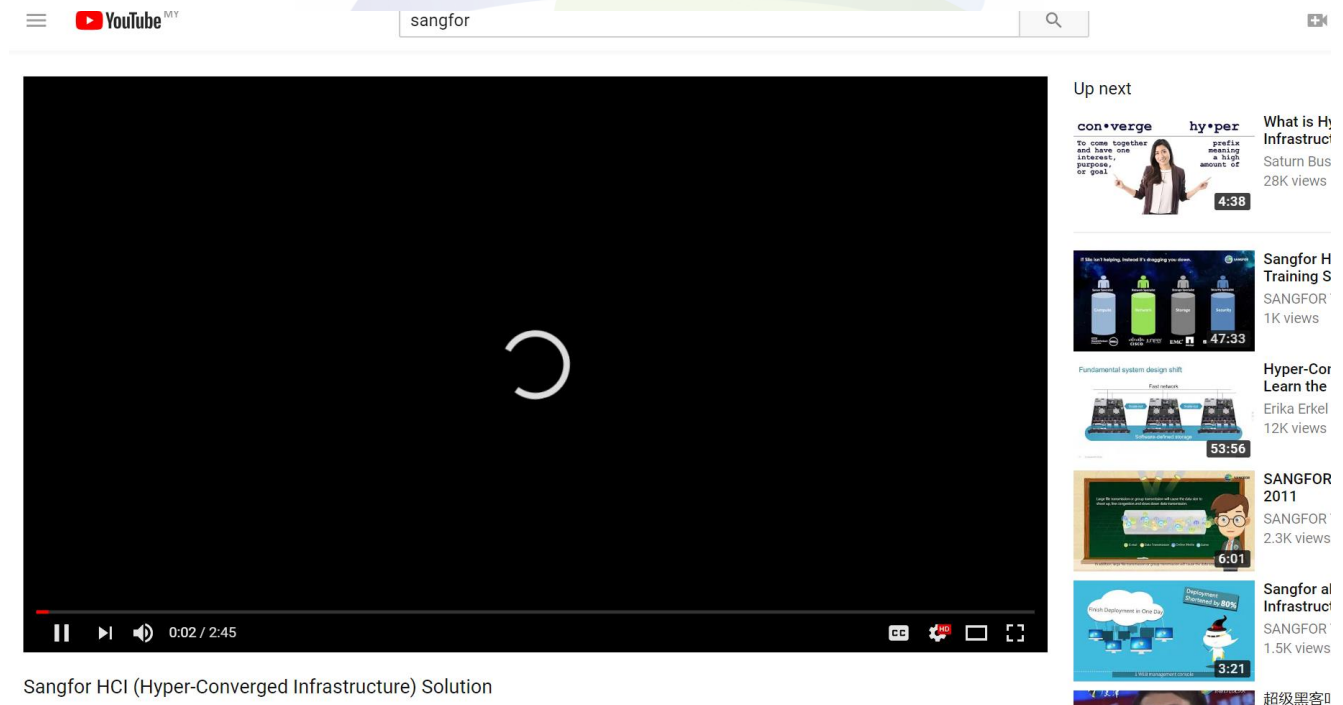


## 4 Test Results

### 4.1 Unable to access online shopping website. (Example: taobao.com )



### 4.2 Failed to watch online streaming media.



## 5 Precautions

- Should not configure LAN users to Global Exclusion in NGAF.
- Application Signature and URL Database must be the latest version.
- If you want to check the log, you can tick “Log Event” in Policy, therefore can check the records in Internal Report Center.

### *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



**SANGFOR**

Content Security (Path: Internal Report Center> Logs>Content Security)  
Application Control (Path: Internal Report Center>Logs>Application Control)



*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](mailto:tech.support@sangfor.com) | W.: [www.sangfor.com](http://www.sangfor.com)