SANGFOR

Sangfor NGAF

Application Control and URL Filtering Configuration Guide

Product Version	8.0.35
Document Version	01
Released on	Jul. 06, 2021

Disclaimer

Products, services or features described in this document, whether wholly or in part, may be not within your purchase scope or usage scope. The products, services or features you purchase must be subject to the commercial contract and terms as agreed by you and Sangfor. Unless otherwise provided in the contract, Sangfor disclaims warranties of any kind, either express or implied, for the content of this document.

Due to product version upgrades or other reasons, the content of this document will be updated from time to time. Unless otherwise agreed, this document is used for reference only, and all statements, information, and recommendations therein do not constitute any express or implied warranties.

Change Log

Date	Change Description
Jul. 06, 2021	This is the first release of this document.

Contents

1 Introduction

1.1 Abbreviations and conventions

NGAF in this article refers to the SANGFOR NGAF device.

1.2 Feedback

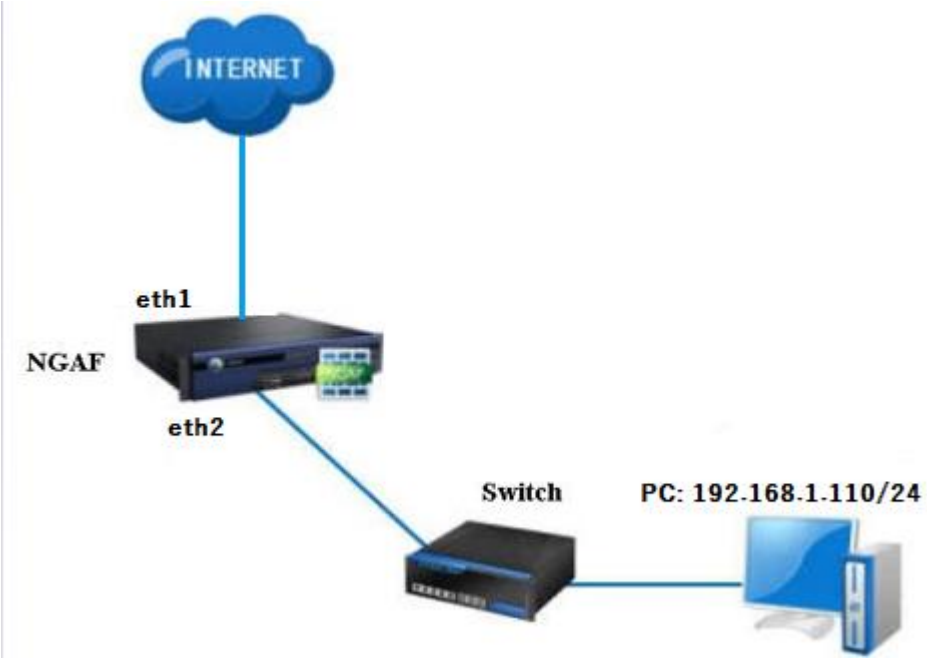
If you find any questions of this documents, please feel free to give us feedback, email: tech.support@sangfor.com.

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 port**: eth1.
- **LAN port**: eth2.
- **LAN PC**: 192.168.1.110/24
- **Deployment**: Route mode.

2.1 Prerequisite

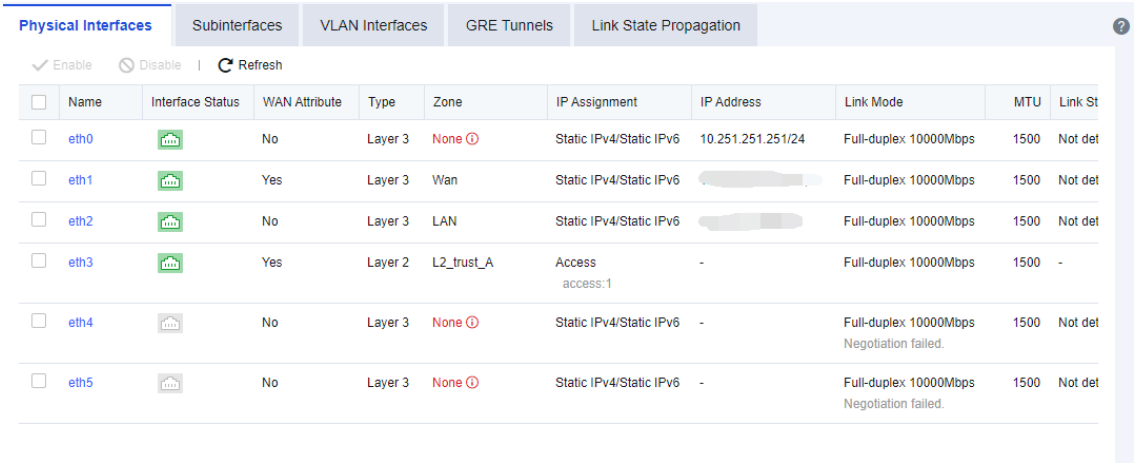
i. Make sure that Application Signature and URL Database upgrade to the latest version.

ii. The data flow of PC accessed to Internet must pass through NGAF.

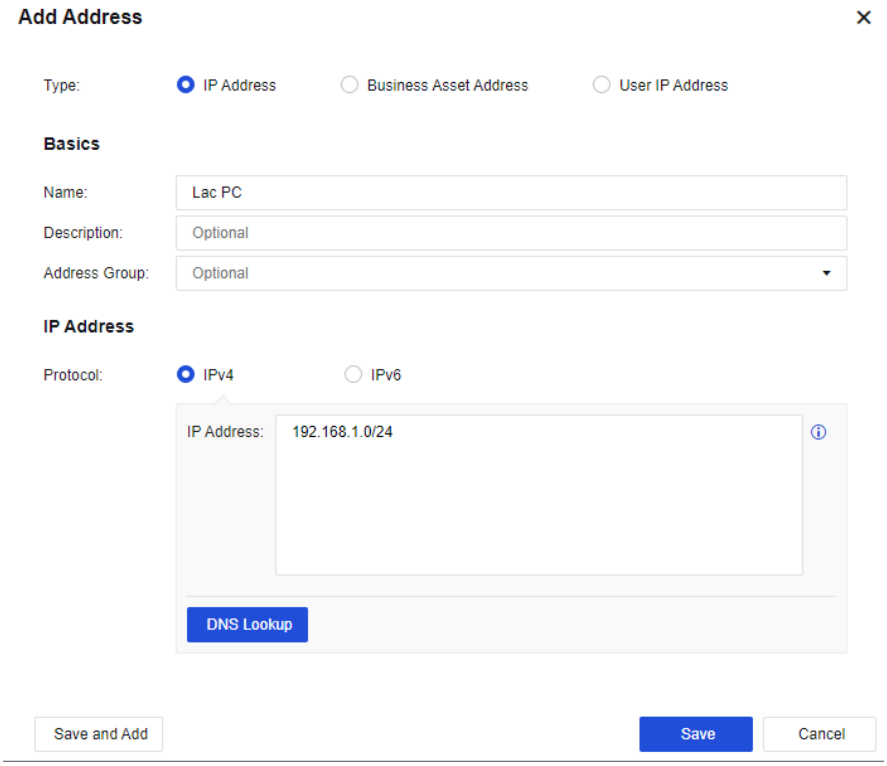
3 Configuration Steps

3.1 Basic setting

Step 1. Login to NGAF web console, configure the types of **eth1** and **eth2** as route mode and in **Network**>**Interfaces**>**Physical Interface**. Besides, configure eth1 as WAN zone with select "**WAN Attribute**" and eth2 as LAN zone.

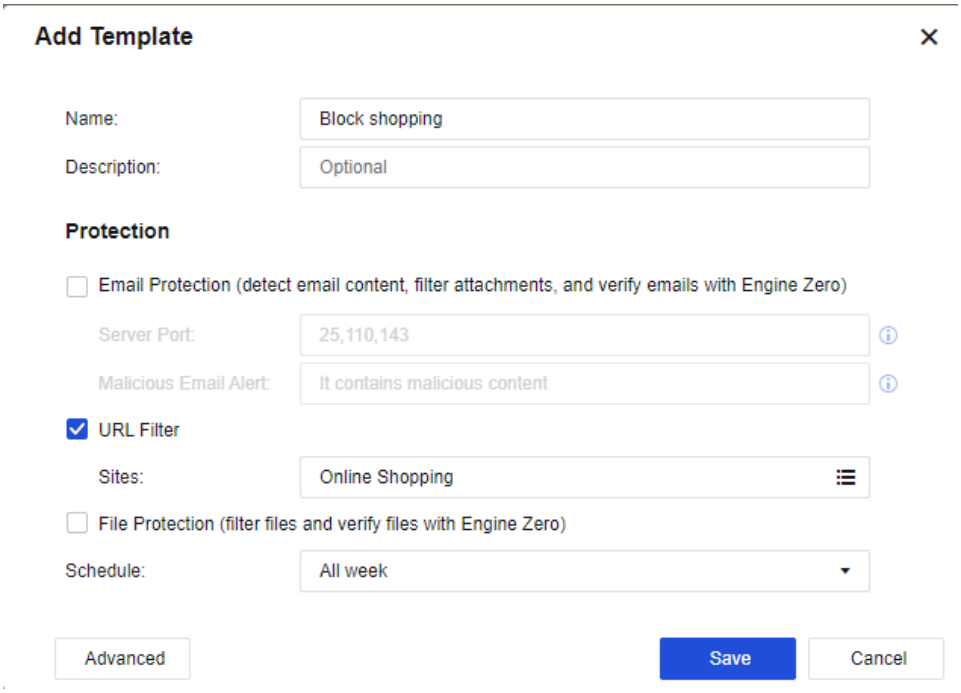


Step 2. In **Objects** > **Network Objects** > **Network Objects** to add "Address" for Lan zone PC with IP address 192.168.1.0/24.

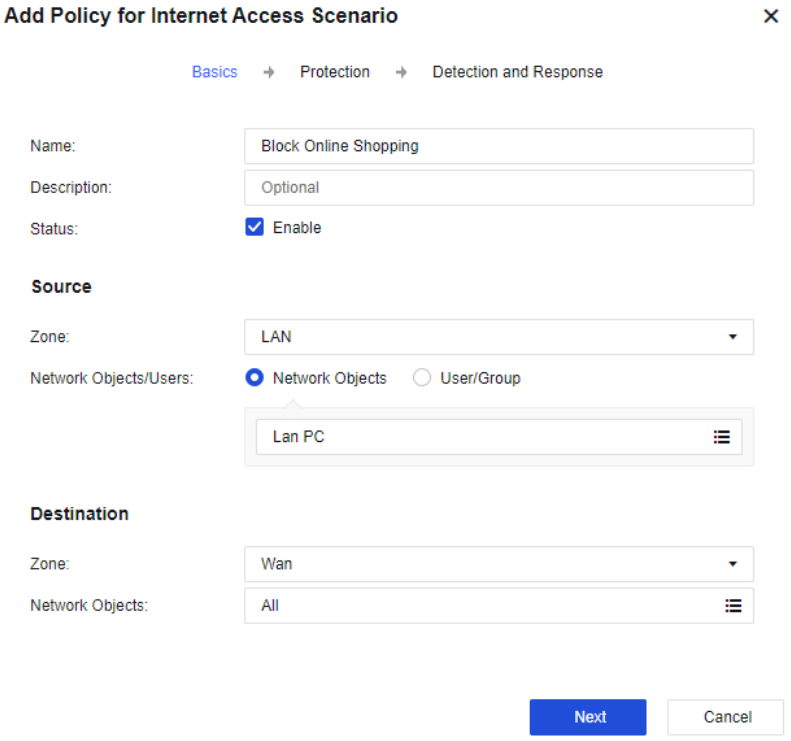


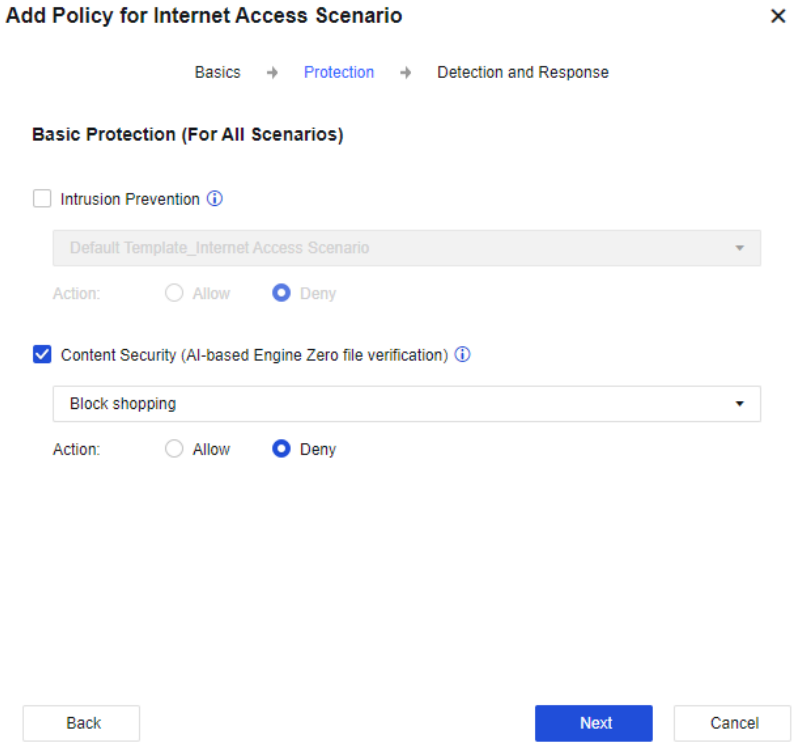
3.2 URL Filtering

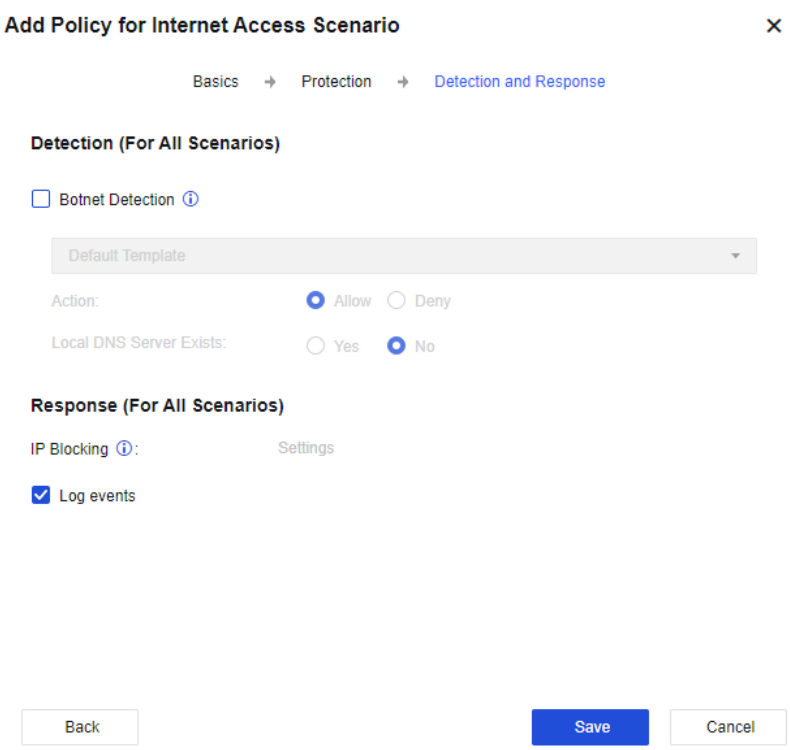
Step 1. In **Objects** > **Security Policy Template** > **Content Security** to create a Content Security Template and select “Online Shopping” in template.

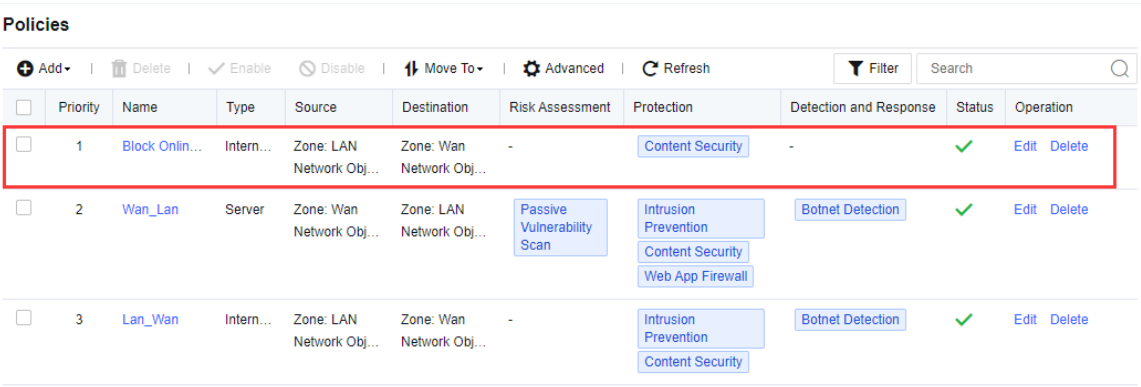


Step 2. In **Policies** > **Network Security** > **Policies**. Create a policy, click **add** > **Policy for Internet Access Scenario** to create a new policy for blocking online shopping.



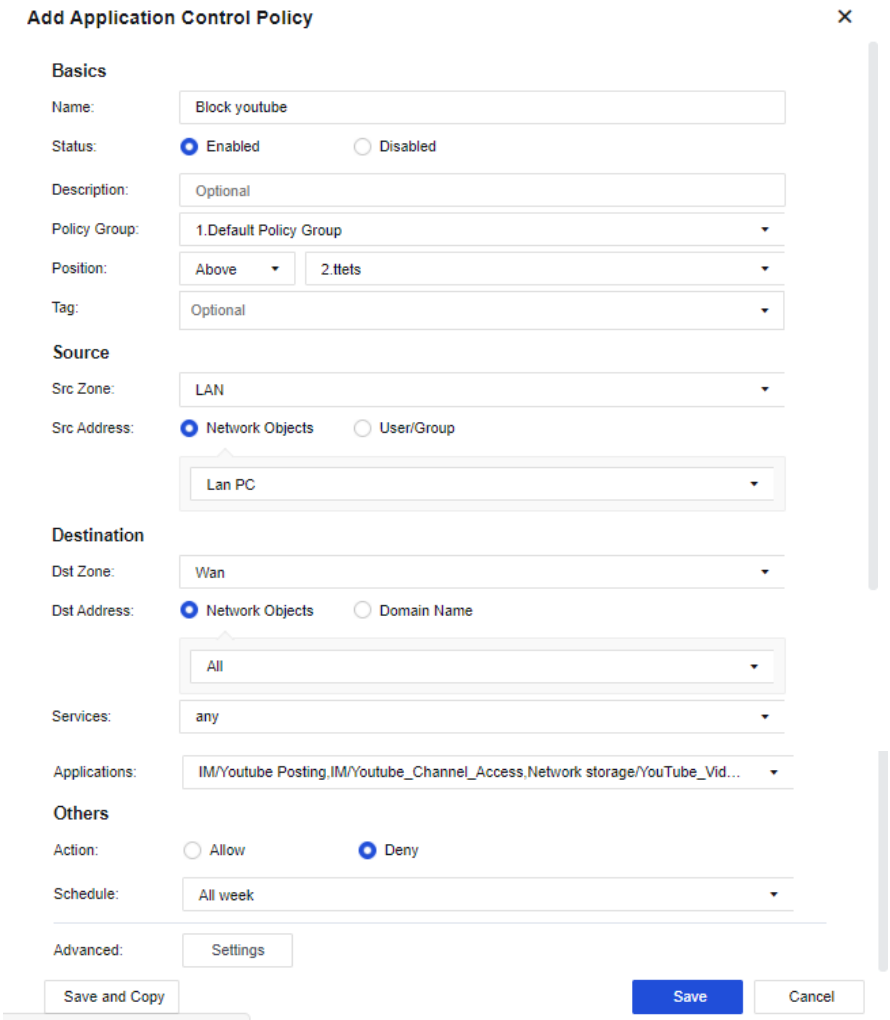



Add Policy for Internet Access Scenario
Basics
Protection
Detection and Response
Detection (For All Scenarios)
Botnet Detection
Default Template
Action:
Allow
Deny
Local DNS Server Exists:
Yes
No
Response (For All Scenarios)
IP Blocking:
Settings
Log events
Back
Save
Cancel


Policies
Add
Delete
Enable
Disable
Move To
Advanced
Refresh
Filter
Search
Priority
Name
Type
Source
Destination
Risk Assessment
Protection
Detection and Response
Status
Operation
1
Block Onlin...
Intern...
Zone: LAN
Network Obj...
Zone: Wan
Network Obj...
-
Content Security
-
Edit
Delete
2
Wan_Lan
Server
Zone: Wan
Network Obj...
Zone: LAN
Network Obj...
Passive Vulnerability Scan
Intrusion Prevention
Content Security
Web App Firewall
Botnet Detection
Edit
Delete
3
Lan_Wan
Intern...
Zone: LAN
Network Obj...
Zone: Wan
Network Obj...
-
Intrusion Prevention
Content Security
Botnet Detection
Edit
Delete

3.3 Application control

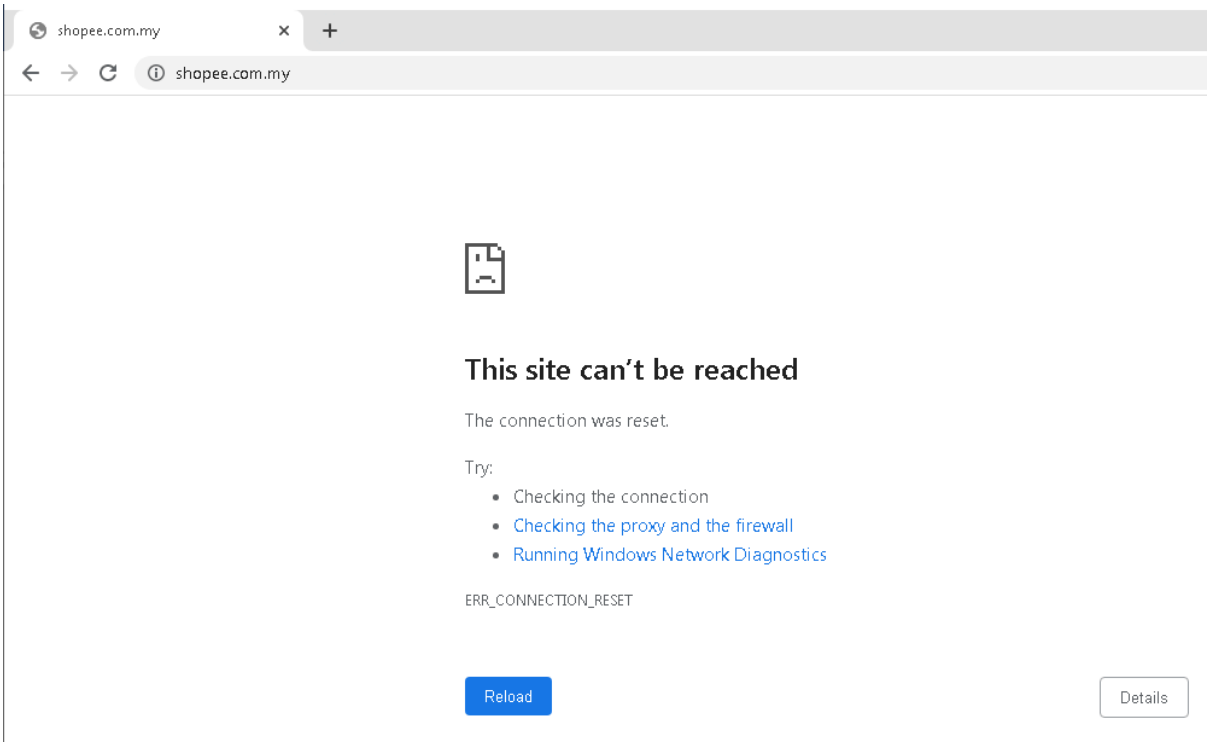
Step 1. In **Policies**>**Access Control**>**Application Control** to create a new policy to restrict users' access YouTube.

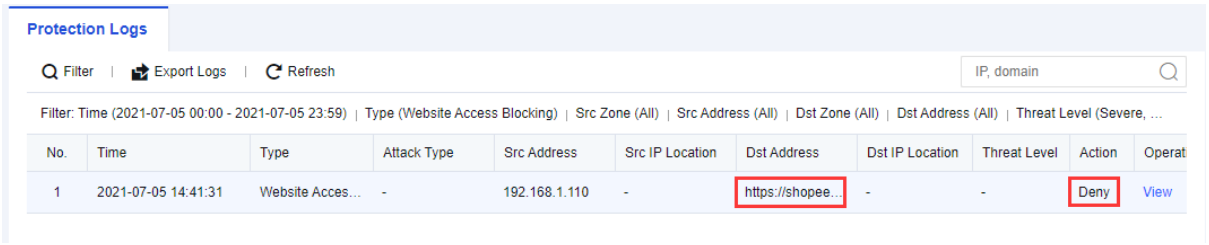


- **Source**
  - ➢ **Src Zone:** Lan zone
  - ➢ **Src Address:** Select Lan PC network object
- **Destination**
  - ➢ **Dst Zone:** Wan zone
  - ➢ **Dst Address:** Select All
- **Services:** Select any
- **Application**: Select all the application which are related with YouTube.

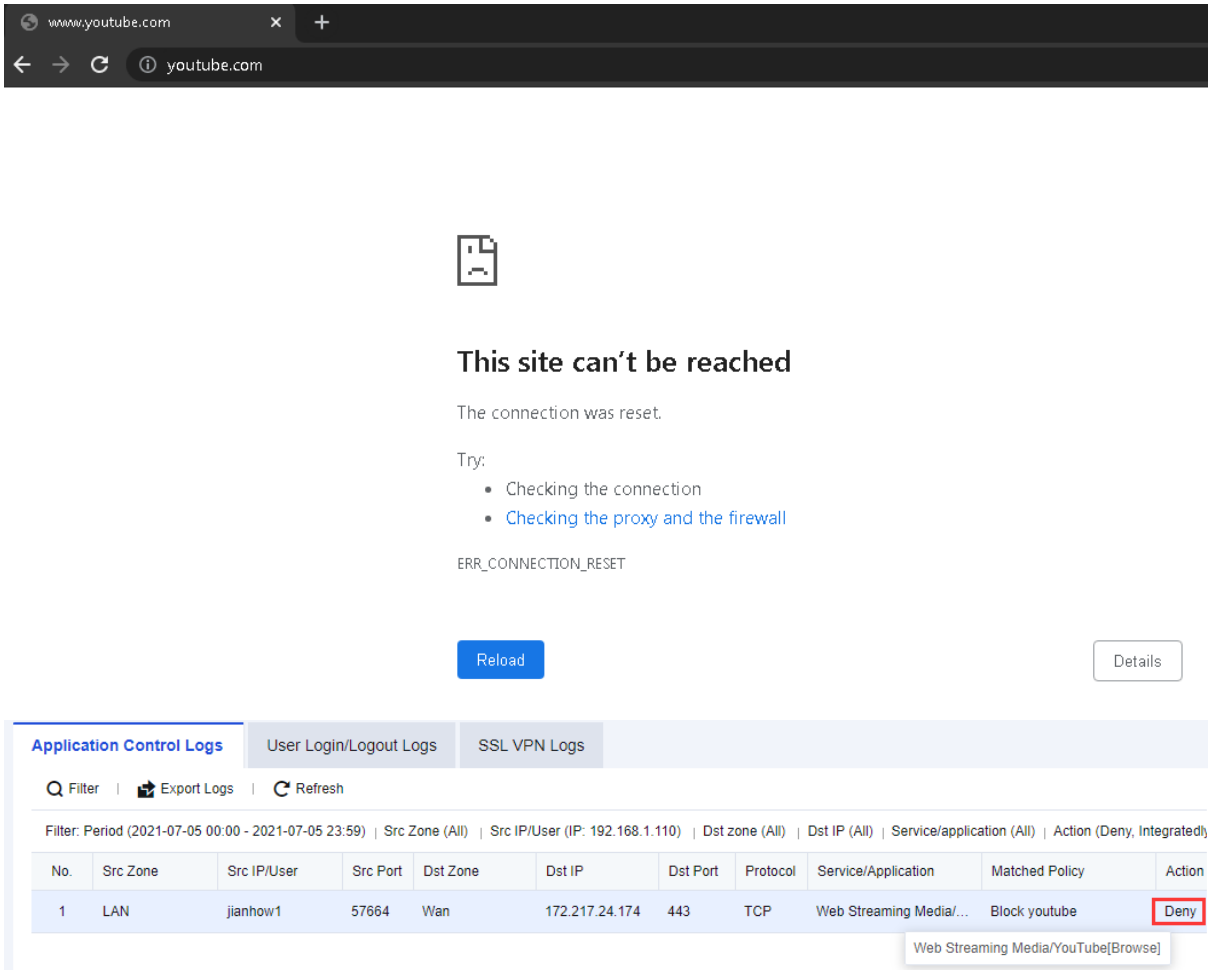
4 Test Results

4.1 Unable to access online shopping website. (Example: shopee.com.my)





4.2 Unable to access YouTube



5 Precautions

i. Should not configure LAN users to **Global Whitelist** in NGAF.

ii. Application Signature and URL Database must be the latest version.

iii. If you want to check the log, you can enable "**Log Event**" in Policy, therefore can check the records in **Monitor.**

- **Content Security** (Path: **Monitor**> **Security Logs**)
- **Application Control** (Path: **Monitor**>**Access Logs**>**Application Control Logs**)

iv. If you found that the URL filtering is not working, you need to clear the browser cache and reopen the browser to test again.

v. If YouTube cannot block through application control policy, you may configure a **custom QUIC service** which are **UDP** port **80** and **443**. Lastly, configure an application control policy and choose the custom service create just now.


SANGFOR