



Sangfor NGAF

Application Control and URL Filtering Configuration Guide

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



Copyright © Sangfor Technologies Inc. 2021. All rights reserved.

Unless otherwise stated or authorized, Sangfor Technologies Inc. (hereinafter referred to as "Sangfor") and its affiliates reserve all intellectual property rights, including but not limited to copyrights, trademarks, patents, and trade secrets, and related rights to text, images, pictures, photographs, audio, videos, charts, colors, and layouts as presented in or concerning this document and content therein. Without prior written consent of Sangfor, this document and content therein must not be reproduced, forwarded, adapted, modified or displayed or distributed by any other means for any purpose.

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

Change Log	1
1 Introduction.....	3
1.1 Abbreviations and conventions	3
1.2 Feedback	3
2 Scenario	4
2.1 Prerequisite	4
3 Configuration Steps.....	5
3.1 Basic setting.....	5
3.2 URL Filtering.....	6
3.3 Application control.....	9
4 Test Results.....	10
4.1 Unable to access online shopping website. (Example: shopee.com.my)	10
4.2 Unable to access YouTube.....	11
5 Precautions.....	12

1 Introduction

1.1 Abbreviations and conventions

NGAF in this article refers to the SANGFOR NGAF device.

1.2 Feedback

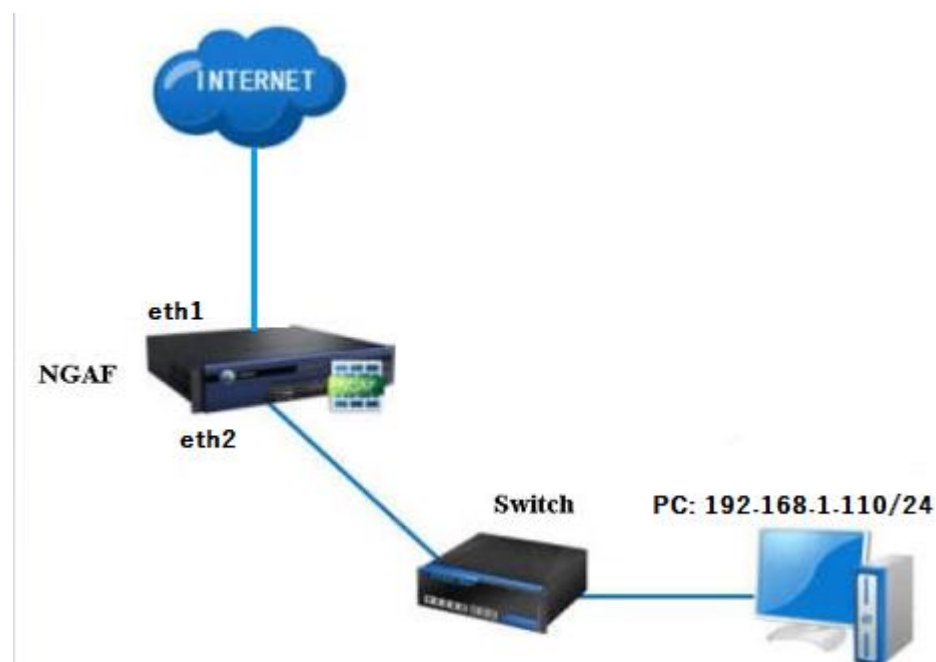
If you find any questions of this documents, please feel free to give us feedback, email: tech.support@sangfor.com.

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.

Physical Interfaces										
Subinterfaces VLAN Interfaces GRE Tunnels Link State Propagation										
<input checked="" type="checkbox"/> Enable <input type="checkbox"/> Disable <input checked="" type="checkbox"/> Refresh										
<input type="checkbox"/>	Name	Interface Status	WAN Attribute	Type	Zone	IP Assignment	IP Address	Link Mode	MTU	Link St
<input type="checkbox"/>	eth0		No	Layer 3	None	Static IPv4/Static IPv6	10.251.251.251/24	Full-duplex 10000Mbps	1500	Not det
<input type="checkbox"/>	eth1		Yes	Layer 3	Wan	Static IPv4/Static IPv6		Full-duplex 10000Mbps	1500	Not det
<input type="checkbox"/>	eth2		No	Layer 3	LAN	Static IPv4/Static IPv6		Full-duplex 10000Mbps	1500	Not det
<input type="checkbox"/>	eth3		Yes	Layer 2	L2_trust_A	Access access:1	-	Full-duplex 10000Mbps	1500	-
<input type="checkbox"/>	eth4		No	Layer 3	None	Static IPv4/Static IPv6	-	Full-duplex 10000Mbps Negotiation failed.	1500	Not det
<input type="checkbox"/>	eth5		No	Layer 3	None	Static IPv4/Static IPv6	-	Full-duplex 10000Mbps Negotiation failed.	1500	Not det

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

Add Address

Type:
 ☒ IP Address
 ☐ Business Asset Address
 ☐ User IP Address

Basics

Name: Lac PC

Description: Optional

Address Group: Optional

IP Address

Protocol:
 ☒ IPv4
 ☐ IPv6

IP Address: 192.168.1.0/24

DNS Lookup

Save and Add

Save

Cancel

Version 01 (Jul.06, 2021)

5

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.

Add Template ×

Name:Block shopping

Description:Optional

Protection

☐ Email Protection (detect email content, filter attachments, and verify emails with Engine Zero)

Server Port:25,110,143 ⓘ

Malicious Email Alert:It contains malicious content ⓘ

☒ URL Filter

Sites:Online Shopping ⓘ

☐ File Protection (filter files and verify files with Engine Zero)

Schedule:All week ▼

Advanced

Save

Cancel

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

Name: Block Online Shopping

Description: Optional

Status: ☒ Enable

Source

Zone: LAN

Network Objects/Users: ☒ Network Objects ☐ User/Group

Lan PC

Destination

Zone: Wan

Network Objects: All

Next

Cancel

Add Policy for Internet Access Scenario ×

Basics → Protection → Detection and Response

Basic Protection (For All Scenarios)

☐ Intrusion Prevention ⓘ

Default Template_Internet Access Scenario

Action: ☐ Allow ☒ Deny

☒ Content Security (AI-based Engine Zero file verification) ⓘ

Block shopping

Action: ☐ Allow ☒ Deny

Back

Next

Cancel

Add Policy for Internet Access Scenario



Basics → Protection → Detection and Response

Detection (For All Scenarios)

☐ Botnet Detection ⓘ

Default Template

Action: ☒ Allow ☐ DenyLocal 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											
<input type="checkbox"/>	Priority	Name	Type	Source	Destination	Risk Assessment	Protection	Detection and Response	Status	Operation	
<input type="checkbox"/>	1	Block Onlin...	Intern...	Zone: LAN Network Obj...	Zone: Wan Network Obj...	-	Content Security	-	✓	Edit	Delete
<input type="checkbox"/>	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
<input type="checkbox"/>	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.

Add Application Control Policy

Basics

Name: Block youtube

Status: ☒ Enabled ☐ Disabled

Description: Optional

Policy Group: 1.Default Policy Group

Position: Above 2.tlets

Tag: Optional

Source

Src Zone: LAN

Src Address: ☒ Network Objects ☐ User/Group

Lan PC

Destination

Dst Zone: Wan

Dst Address: ☒ Network Objects ☐ Domain Name

All

Services: any

Applications: IM/Youtube Posting,IM/Youtube_Channel_Access,Network storage/YouTube_Vid...

Others

Action: ☐ Allow ☒ Deny

Schedule: All week

Advanced: Settings

Save and Copy Save Cancel

- **Source**

- **Src Zone:** Lan zone

- **Src Address:** Select Lan PC network object

- **Destination**

- **Dst Zone:** Wan zone

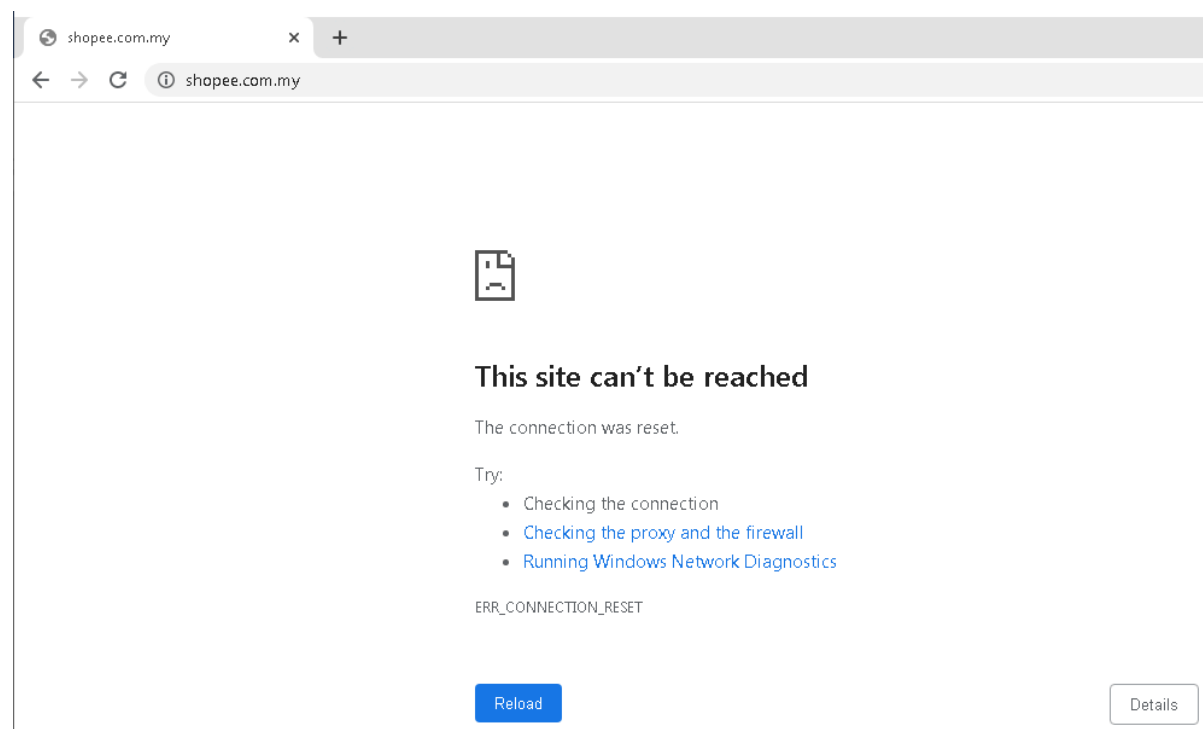
- **Dst Address:** Select All

- **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)



shopee.com.my

← → ↻ ⓘ shopee.com.my



This site can't be reached

The connection was reset.

Try:

- Checking the connection
- [Checking the proxy and the firewall](#)
- [Running Windows Network Diagnostics](#)

ERR_CONNECTION_RESET

[Reload](#) [Details](#)

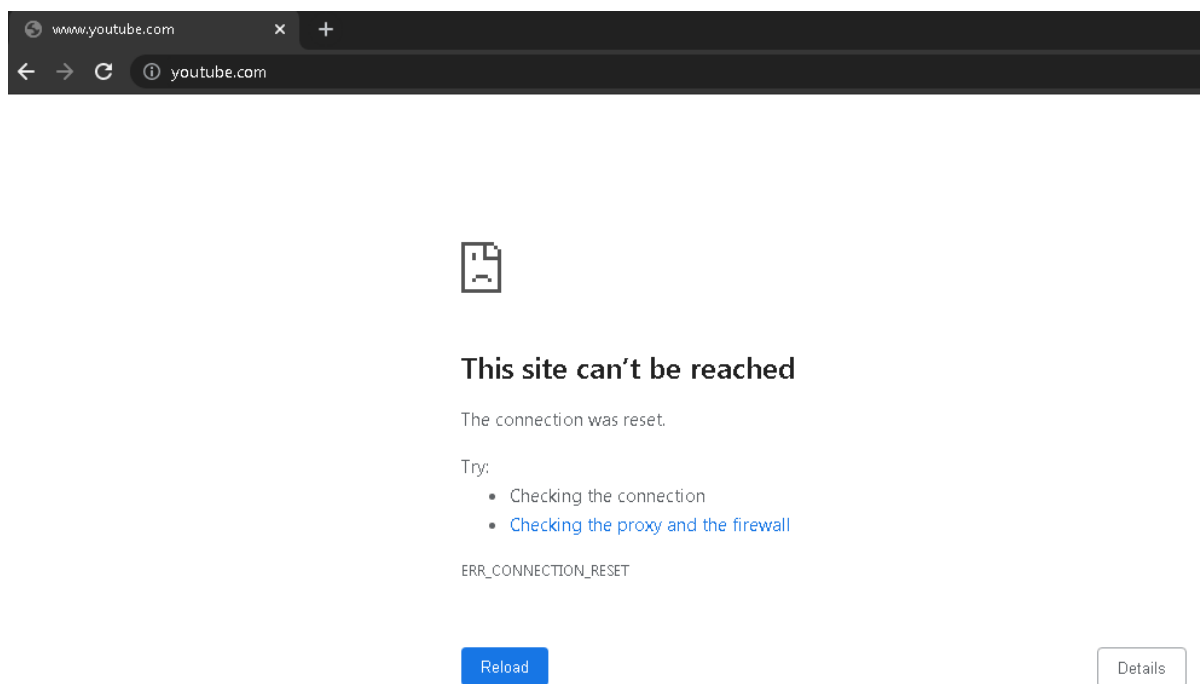
Protection Logs

Filter | Export Logs | Refresh

Filter: Time (2021-07-05 00:00 - 2021-07-05 23:59) | Type (Website Access Blocking) | Src Zone (All) | Src Address (All) | Dst Zone (All) | Dst Address (All) | Threat Level (Severe, ...)

No.	Time	Type	Attack Type	Src Address	Src IP Location	Dst Address	Dst IP Location	Threat Level	Action	Operat
1	2021-07-05 14:41:31	Website Acces...	-	192.168.1.110	-	https://shopee...	-	-	Deny	View

4.2 Unable to access YouTube



This site can't be reached

The connection was reset.

Try:

- Checking the connection
- [Checking the proxy and the firewall](#)

ERR_CONNECTION_RESET

[Reload](#) [Details](#)

Application Control Logs | User Login/Logout Logs | SSL VPN Logs

Filter | Export Logs | Refresh

Filter: Period (2021-07-05 00:00 - 2021-07-05 23:59) | Src Zone (All) | Src IP/User (IP: 192.168.1.110) | Dst zone (All) | Dst IP (All) | Service/application (All) | Action (Deny, Integrated)

No.	Src Zone	Src IP/User	Src Port	Dst Zone	Dst IP	Dst Port	Protocol	Service/Application	Matched Policy	Action
1	LAN	jianhow1	57664	Wan	172.217.24.174	443	TCP	Web Streaming Media/...	Block youtube	Deny

Web Streaming Media/YouTube[Browse]

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

