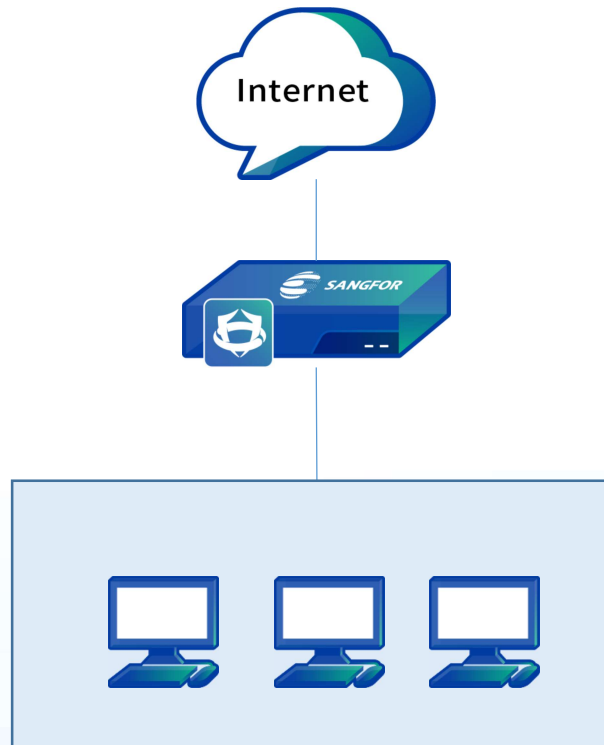


# URL Filtering - Configuration Guideline



Company B has purchased a NSF and deployed as gateway. Besides blocking the access for counteraction, illegal website, customer also wish to block the access to microblog and <http://game.baidu.com>



# URL Filtering - Configuration Steps



1. In **Object > Content Identification Database > URL Category**, add a new self-define URL category and fill in the self-defined URL(game.baidu.com)

The screenshot displays the Sangfor management console interface for URL filtering. On the left, a sidebar menu shows the navigation path: **Objects** > **Content Identification Database** > **URL Category**. The main panel shows a table of predefined URL categories. A modal dialog titled "Add URL Category" is open in the foreground, allowing for the creation of a custom category. The fields in the dialog are as follows:

Field	Value
Name	Game2
Description	Optional
URL	game.baidu.com
URL Keyword	Optional

The background table lists predefined categories such as "Job-hunting & Employment", "Adult Content", "Online Shopping", "News Portal", "IT Related", "Education", "Religion", "Nonprofit Organization", "Science & Technology", "Web Application", and "Illegality & Immorality". Each entry includes a checkbox, a description, a type (Predefined), and edit/delete actions.

# URL Filtering - Configuration Steps



2. In **Objects > Security Policy Template > Content Security**, add a new template, in URL filtering select the respective website category.

The screenshot displays the Sangfor Security Management System interface. On the left, the 'Objects' sidebar is visible, with 'Security Policy Template' selected. The main area shows the 'Content Security' configuration page. A table lists existing templates, including 'Default Template' and 'Anti-ransomware via file'. An 'Add Template' dialog is open, showing fields for Name, Description, and Protection settings. The 'URL Filter' checkbox is checked. A 'URL Category' selection window is also open, showing a list of categories. The 'Game2' category is selected, and the 'Save' button is highlighted.

No.	Name	Email Protection	URL Filter	File Protection	In Use
1	Default Template	Enable	Enable	Enable	None
2	Anti-ransomware via file				None
3	Default Template_Intern				
4	Default Template_Serve				

**Add Template**

Name:

Description:

**Protection**

- ☒ Email Protection (detect email content, filter attachments)
- Server Port:
- Malicious Email Alert:
- ☒ URL Filter
- Sites:
- ☒ File Protection (filter files and verify files with engines)
- Schedule:

**URL Category**

All

- ☐ Finance
- ☐ Entertainment
- ☐ Policy & Law
- ☐ Business & Economy
- ☐ Network Security
- ☐ Software Update
- ☐ Malware
- ☐ Malicious Script
- ☒ Game2
- ☐ Uncategorized

Selected (1)

Game2

# URL Filtering - Configuration Steps



3. In **Policy > Network Security > Policies**, add a new policy for internet access scenario. LAN zone and LAN subnet was selected as source, All network segment and WAN zone was selected as destination. Select the content security template from steps 2, other security protection may enable based on your needs.

**Add Policy for Internet Access Scenario**

Basics → Protection → Detection and Response

**Basics**

Name: Deny

Description: Optional

Status: ☒ Enable

**Source**

Zone: lan

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

Private Network Segment

**Destination**

Zone: wan

Network Objects: All

**Protection**

**Basic Protection (For All Scenarios)**

☒ Intrusion Prevention ⓘ

Default Template\_Internet Access Scenario

Action: ☐ Allow ☒ Deny

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

Deny

Action: ☐ Allow ☒ Deny

Back Next Cancel

## URL Filtering – Precautions



1. Single arm mode does not support URL filtering
2. URL filtering is based on domain checking. It does not conflict with the detection method of WAF.
3. In order to achieve better filtering effect, the URL database needs to be kept up to date.