Grandstream Networks, Inc.

GWN700x

Content Security Guide

GWN700x - Content Security Guide

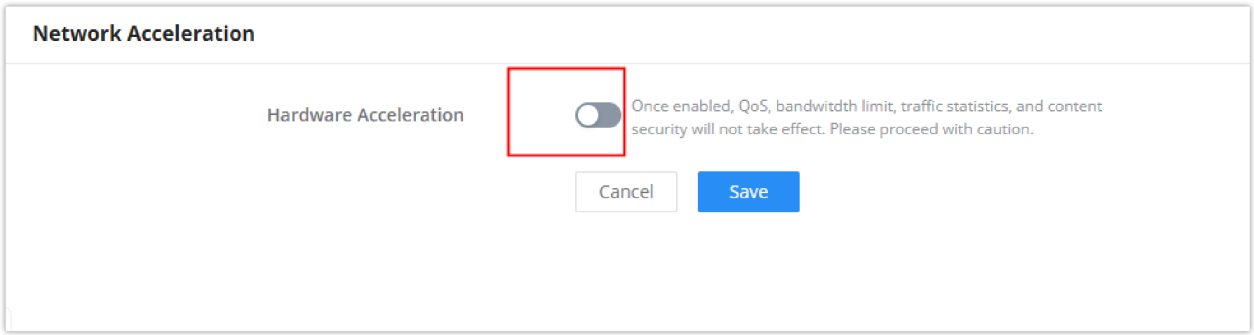
Overview

This document describes how to configure Content Security for the GWN700X device. The content security will include features to restrict access to specific websites, using different methods, such as DNS Filtering, URL Filtering, and Application Filtering, in this guide, we will walk through these different approaches, and how they can be configured.

Preconditions

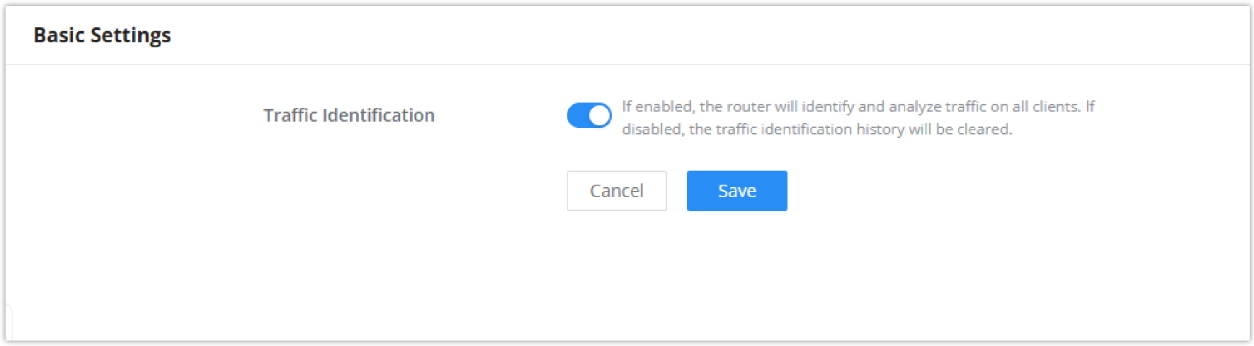
Before configuring any of the content security features, make sure to apply the following changes:

- Disabling Hardware Acceleration, Under **Network Settings** → **Network Acceleration**.



Hardware Acceleration

- Enabling Traffic Identification, Under **Traffic Management** → **Basic Settings**.



Traffic Identification

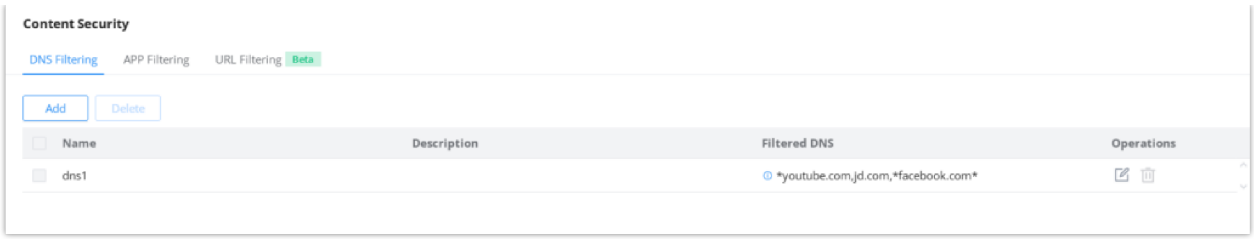
Configure Content Security Rules

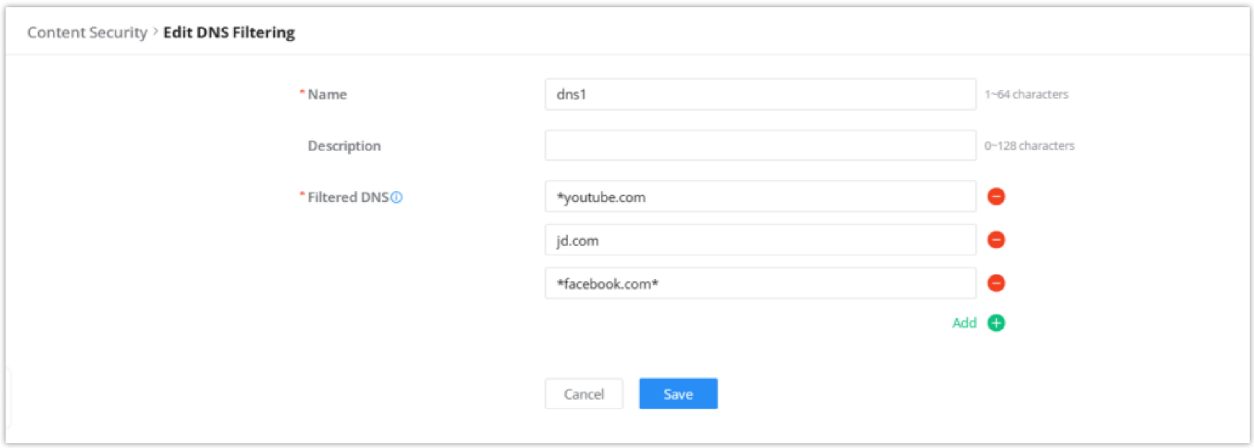
The **Content Security** feature allows you to restrict user access to specific online content and applications, enhancing network security. To implement this, you will need to set up filtering rules and bind them to your firewall's traffic policies. This section will walk you through the process of using **DNS Filtering**, **APP Filtering**, and **URL Filtering** to control access and ensure your network's safety.

DNS Filtering Rules

Please follow the below steps to configure a DNS Filtering rule:

1. Enter the content security page, select DNS filtering, and add a rule.
2. Input a name for the DNS Filter rule.
3. DNS filter supports wildcard pattern matching, Example: DNS 1: added * Baidu. Com *.
4. Once the rule is saved, users cannot access all pages that contain Baidu.com.





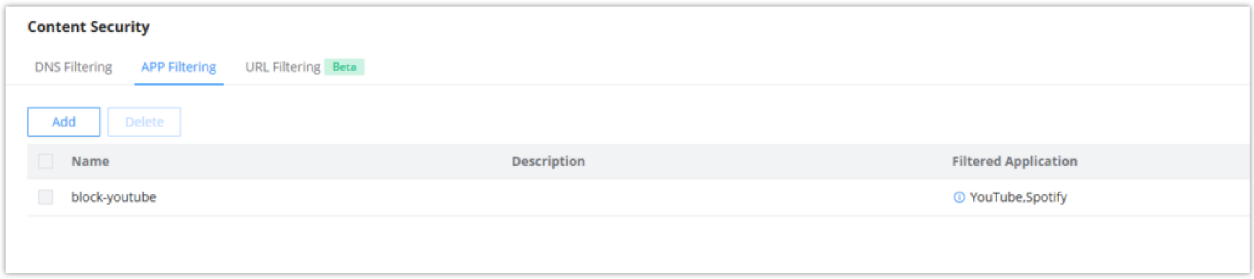
Note

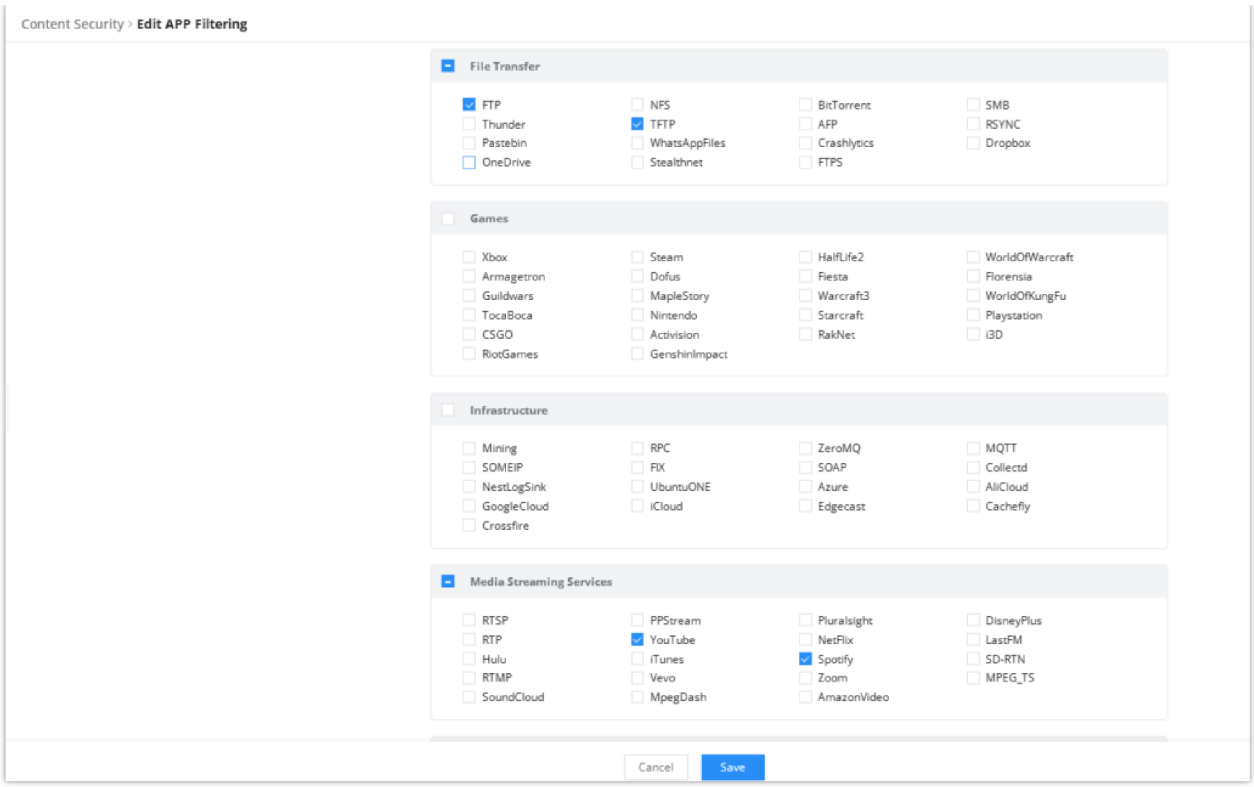
For the DNS Filtering to work, it will require the connected client to have the IP address of the gateway, as its DNS server

APP Filtering Rules

To create an Application Filtering rule, Please follow the below steps:

1. Enter the **Content Security** → **APP Filtering** page to add a rule.
2. Enter a name and select the application, or the application protocol to be blocked or Multiple selections and deselection are supported.
3. App filtering will prohibit access to web pages for YouTube and Spotify.

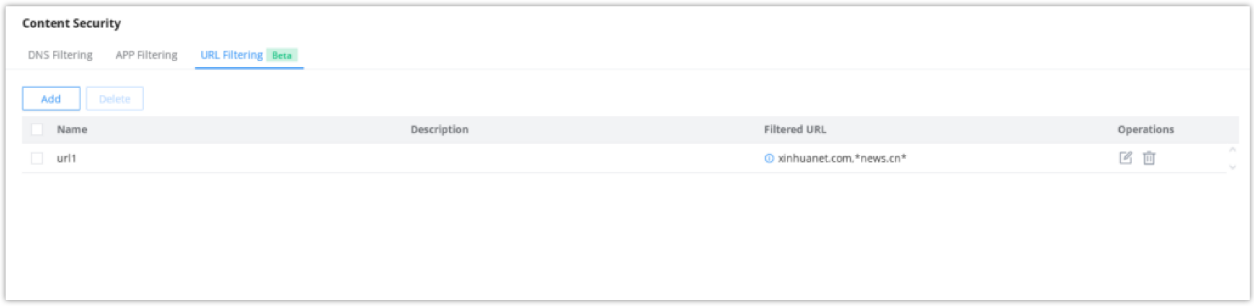


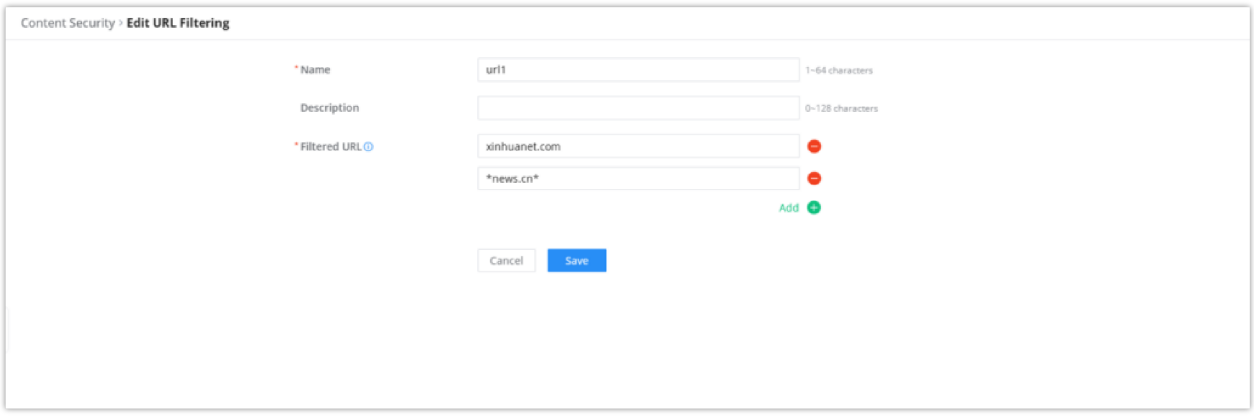


URL filtering Rules

To create a URL Filtering Rule, please follow the below steps:

1. Go to the content security-URL Filtering page and add a rule.
2. Enter name and Filtered URL. Filtered URL supports wildcard matching.
3. URL Filtering will not block HTTPS Traffic, only HTTP blocking, Example: URL 1: added * xinhuanet.com *, this is an example of an insecure HTTP website.
4. Users are prevented from accessing all HTTP pages that contain xinhuanet.com.



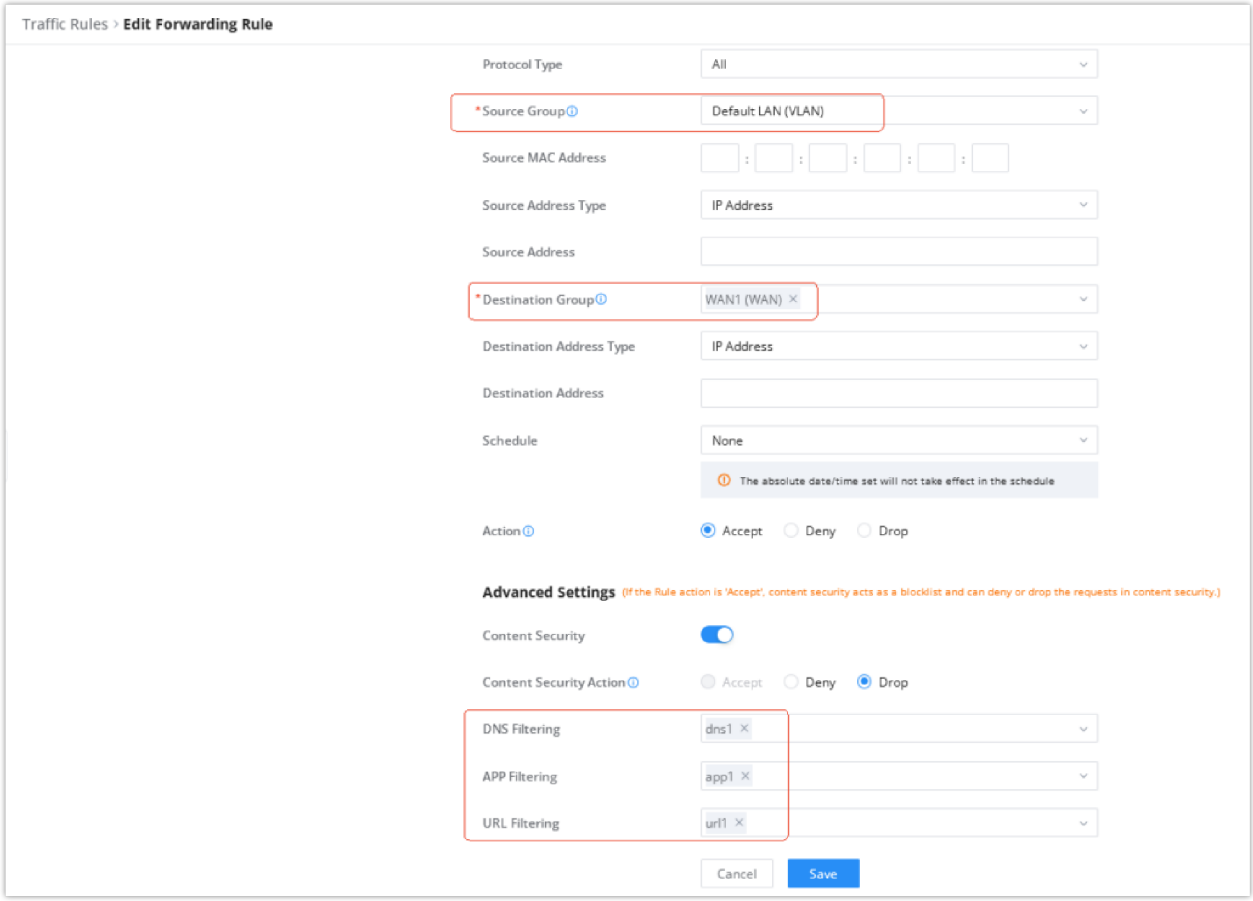


Content Filtering through Firewall Rules

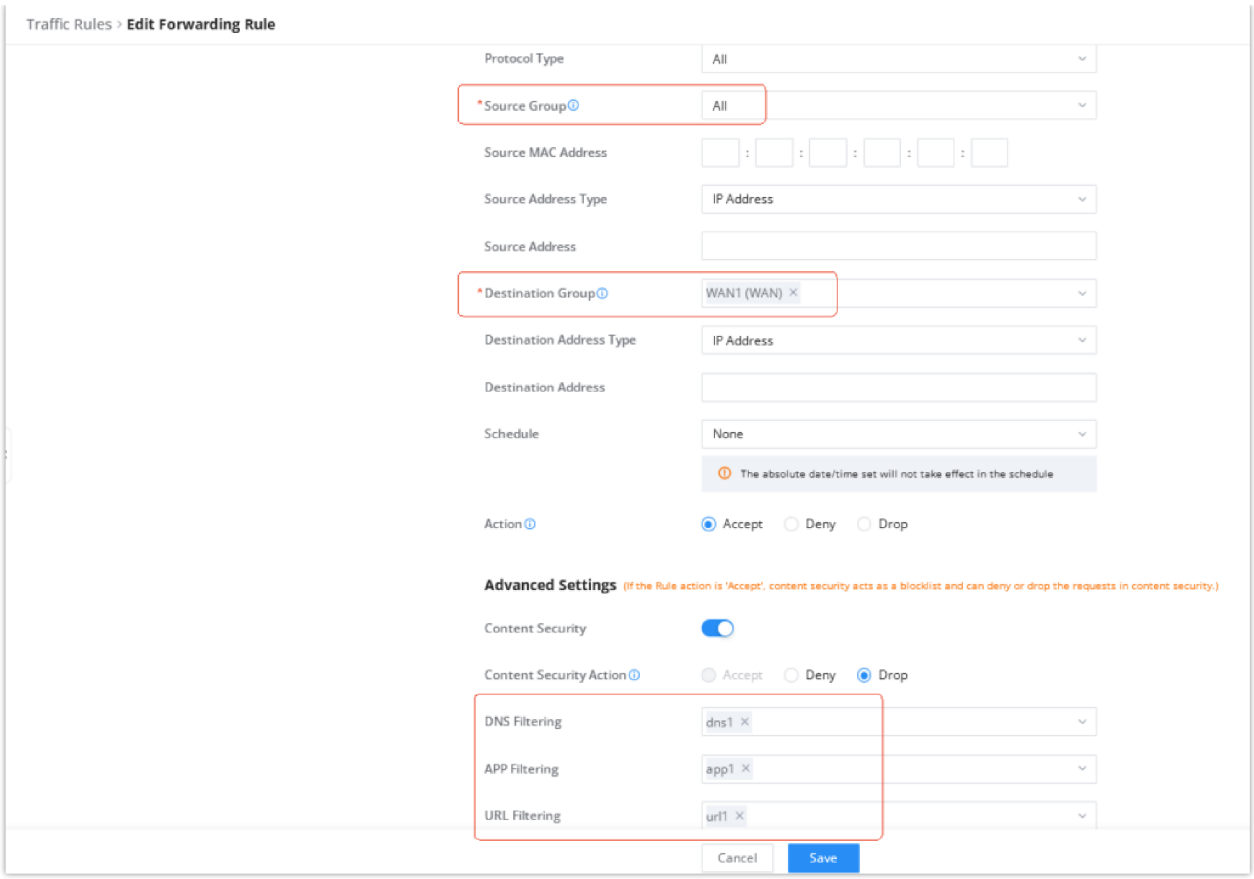
Block user access to certain DNS/APP/URL

The content filtering can be achieved by creating Firewall rules, for incoming/Outgoing traffic, let's take a look at the example below:

- Go to Traffic Rules, add a Forwarding Rule, and enable this rule.
- Choose your Source Group and Destination Group.
- Action select Accept, Enable Content Security, Content Security Action select Deny/Drop, Bind DNS Filtering/APP Filtering/URL Filtering as required.



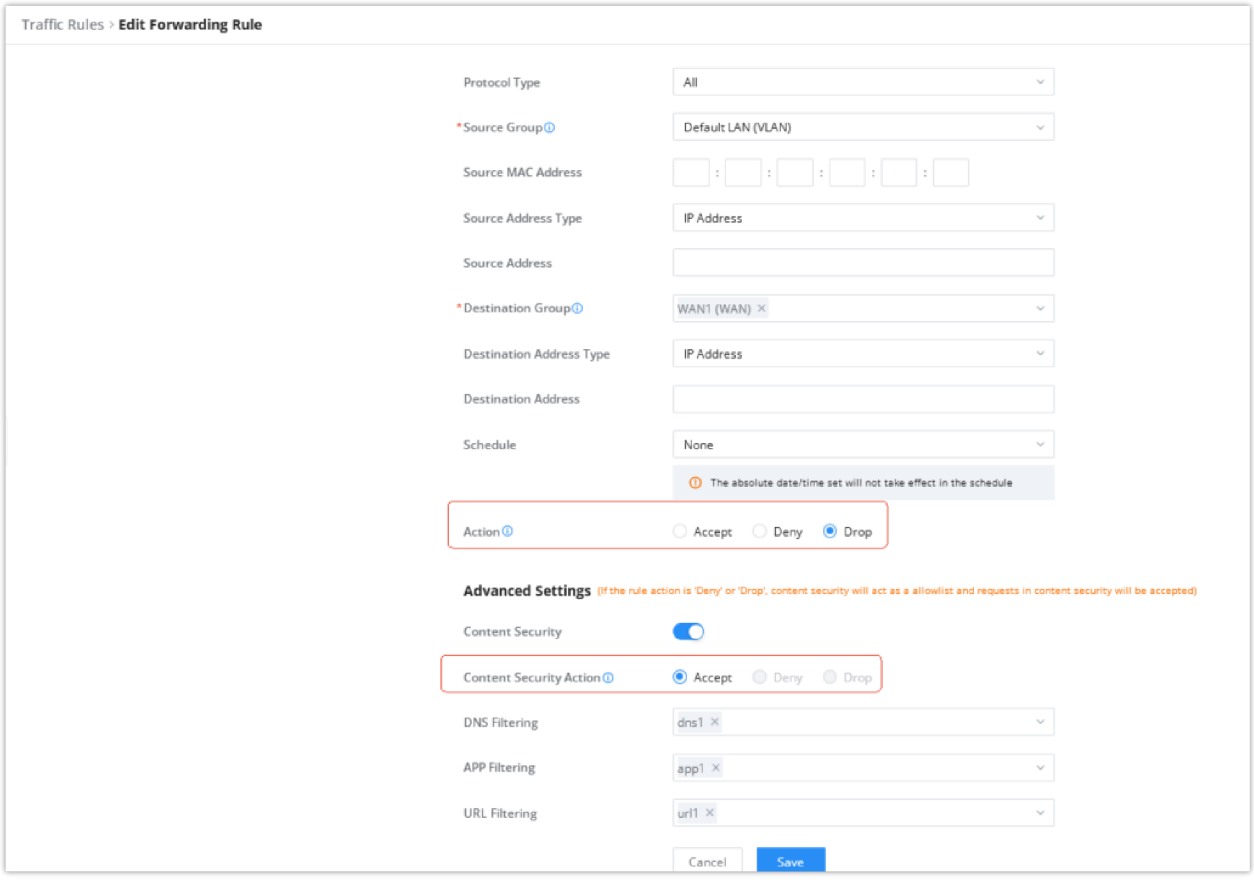
- All VLAN content restrictions, Select all for the source group.



- Blocked DNS/URL pages cannot be loaded and Blocked apps cannot use basic functions.

Block user access to traffic outside of content security

- User access to non-content-controlled traffic is prohibited, Example: Only default VLAN users are allowed to access DNS1, APP1, URL1, and other traffic is Deny/Drop.



Supported Devices

Product	Minimum Firmware Required
GWN7001	1.0.1.6
GWN7002	1.0.1.6
GWN7003	1.0.1.6

Content Security Supported Devices

Need Support?

Can’t find the answer you’re looking for? Don’t worry we’re here to help!

CONTACT SUPPORT