

# Grandstream Networks, Inc.

GWN700x Series GWN700x – Firewall Content Security



The content security feature on GWN700x routers allows users to filter (block) content based on DNS, APP or URL. DNS and URL filtering uses keywords and wildcard \* (which can represent any string) while APP filtering works by selecting APPs from a list organized in categories.

To filter (block) content please follow the steps below:

### **Disable Hardware Acceleration**

Navigate to Web UI → Network Settings → Network Acceleration, then toggle OFF "Hardware Acceleration".

Network Acceleration			
Hardware Acceleration	Once er IPSec Cl	abled, QoS, rate limit, traffic statistic ent-to-Site will not take effect. Pleas	, content security and e proceed with caution.
	Cancel	Save	
	Hardware Ac	celeration	

### **Enable Traffic Identification**

Navigate to Web UI → Traffic Management → Basic Settings, then toggle ON "Traffic Identification".

Basic Settings	
Traffic Identification	If enabled, the router will indentify and analyze traffic on all clients. If disabled, the traffic identification history will be cleared.
	Cancel Save
	Traffic Identification

## Add a Content Security Filter

Navigate to **Web UI**  $\rightarrow$  **Firewall**  $\rightarrow$  **Content Security**, click on DNS Filtering, APP Filtering or URL Filtering tab, then click on "Add" button to add a new filter.

Content Security					
DNS Filtering APP Filtering		URL Filtering Beta			
Add	Delete				
Name		Description			
youtube.	com	youtube			



**Example:** DNS Filtering for media streaming, click on "minus" or "plus" icons to add or remove an entry, refer to the figure below:

#### Note:

Enter keywords and wildcard characters \* (which can represent any string). Wildcard \* can only be added before or after the input keyword, for example: \*.imag, news\*, \*news\*. Please enter a valid domain name, not an IP address.

Content Security > Add DNS Filtering							
*Name	Media Streaming	1~64 characters					
Description	Filter media streaming	0~128 characters					
*Filtered DNS ①	*youtube.com*	•					
	*netflix.com*	•					
	Please Enter	•					
		Add \pm					
	Cancel Save						

Add DNS Filtering

**Example:** APP Filtering for streaming APPS, select multiple APPs/Services or select the whole category, refer to the figure below:

	ormation				
*Name		Streaming AF	PPs		1~64 characters
Description	n	Filtering med	ia streaming services		0–128 characters
Filtered /	Application				
	Application				
	fficiently identifiab	le Others			
All E	fficiently identifiab	le Others			
All E	fficiently identifiab	le Others			
All E Media Strea	fficiently identifiab	le Others	Pluralsight	Disney	Plus
All E Media Strea RTSP RTP	fficiently identifiab	le Others PPStream YouTube	Pluralsight	Disney	Plus 1
All E Media Strea RTSP RTP Hulu	fficiently identifiab	le Others PPStream YouTube iTunes	<ul> <li>Pluralsight</li> <li>✓ NetFix</li> <li>Spotify</li> </ul>	Disney LastFM SD-RTM	Plus 1
All E Media Strea RTSP Hulu RTMP	fficiently identifiab	PPStream YouTube iTunes Vevo	Pluralsight	Disney LastFM SD-RTM MPEG_	Plus 1 N TS

Add APP Filtering

**Example:** URL Filtering for media streaming, click on "minus" or "plus" icons to add or remove an entry, refer to the figure below:

#### Note:

Only unencrypted HTTP pages/requests are supported. HTTPS is not supported.

*Name	URL Filtering	1~64 characters
Description	Media streaming	0~128 characters
*Filtered URL ①	*.imag	•
	news*	•
	*news*	•
	Please Enter	•
		Add \pm
	Cancel	
	Add URL Filtering	

# Add a Traffic Rule

Note:

• If the client's devices are using the default DNS Server of the GWN700x router, in this case, the DNS traffic is handled by "Inbound Rules".

Navigate to **Web UI**  $\rightarrow$  **Firewall**  $\rightarrow$  **Traffic rules**, click on **Inbound Rules** tab, then click on "**Add**" icon to add a new Inbound rule, scroll down and enable "**Content Security**" then select the previously created filters from the drop-down list under DNS Filtering, APP Filtering and URL Filtering accordingly, refer to the figure below:

	*Name	Media streaming Inbound rule		1~64 characters
	Status			
	IP Family	Any IPv4 IPv6		
	Protocol Type	All	v	
	*Source Group ①	Default (VLAN)	~	
	Source MAC Address			
	Source IP Address			Enter the IP address/mask length, such a "192,168.122.0/24"
	Destination IP Address			Enter the IP address/mask length, such a "192.168.122.0/24"
	Destination IP Address	Accept Deny Drop		Enter the IP address/mask length, such a "192.168.122.0/24"
г	Destination IP Address Action Action	Accept Deny Drop  action is "Accept. content security acts as a blocklist and can deny or drop	the reque	Enter the IP address/mask length, such a "192.168.122.0/24"
	Destination IP Address Action () Advanced Settings () The Rule of Content Security	Accept Deny Drop  action is 'Accept', content security acts as a blockist and can deny or drop t	the reque	Enter the IP address/mask length, such a "192.168.122.0/24"
[	Destination IP Address Action (*) Advanced Settings (*) the Rule : Content Security Content Security Action (*)	Accept Deny Drop  action is 'Accept', content security acts as a blocklist and can deny or drop t      Accept Deny Drop	the reque	Enter the IP address/mask-length, such a *192.168.122.02.04 sists in content security.)
	Destination IP Address Action Advanced Settings (If the Rule a Content Security Content Security Action DNS Filtering	Accept Deny Drop  action is Accept. Ontent security acts as a blocklist and can deny or drop t  Accept Deny Oprop  DNS Filter x	the reque	Enter the IP address/mask length, such a "192,168,132,0024"
	Destination IP Address Action Advanced Settings of the Rule: Content Security Content Security Action DNS Filtering APP Filtering	Accept Deny Drop  action is 'Accept. Content security acts as a blocklist and can deny or drop t      Accept Deny Drop      DNS Filter ×      APP Filter ×	the reque	Enter the IP address/mask length, such a
	Destination IP Address Action Action Advanced Settings of the Rule: Content Security Content Security Content Security Action DNS Filtering URL Filtering URL Filtering	Accept Deny Drop  action is 'Accept. Content security acts as a blocklist and can deny or drop of  Accopt Deny Drop  DNS Filter ×  APP Filter  APP Filter	the reque	Enter the IP address/mask length, such a

Add Inbound Rule

Navigate to **Web UI**  $\rightarrow$  **Firewall**  $\rightarrow$  **Traffic rules**, click on **Forwarding Rules** tab, then click on "**Add**" icon to add a new forwarding rule, scroll down and enable "**Content Security**" then select the previously created filters from the drop-down list under DNS Filtering, APP Filtering and URL Filtering accordingly, refer to the figure below:

*Name	Media Streaming Forwarding Rule	1~64 characters
Status		
IP Family	Any ○ IPv4 ○ IPv6	
Protocol Type	All	v.
*Source Group ③	Default (VLAN)	~
Source MAC Address		
Source IP Address		Enter the IP address/mask length, such a "192.168.122.0/24"
*Destination Group	wan) $\times$ (NAW) EVAW	~
Destination IP Address		Enter the IP address/mask length, such a "192.168.122.0/24"
Action ()	Accept O Deny O Drop	
Advanced Settings Of the Ru Content Security	e action is 'Actept', content security acts as a blocklist and can deny or drop	the requests in content security.)
Content Security Action ③	Accept O Deny  O Drop	
DNS Filtering	DNS Filter ×	~
	APP Filter ×	~
APP Filtering		

Add Forwarding Rule

Make sure to place the rule on top of all rules (top of the list), refer to the figure below:

Traff	fic Rules										
Inbo	ound Rules Out	bound Rules	Forwarding Rules								
A	dd Delete								All Source	Groups	~
	Name	Status	IP Family	Protocol Type	Source Group	Source MAC Address	Source IP Address	Source Po	rt Des	Operations	
	Media stream		Any	All	Default (VLAN)					≐ ⊠ ⊡	
	Anti-lockout-R		Any	ТСР	Default (VLAN)					≑ ☑ 亩	
	WAN2_Allow		IPv4	UDP	WAN3 (WAN)	-	-	-		≐ ☑ 亩	
	WAN2_Allow		IPv4	ICMP	WAN3 (WAN)			-	-	≑ ☑ ⊡	
	WAN2_Allow-I		IPv4	IGMP	WAN3 (WAN)			1		≡ 🗹 🖻	
	WAN2_Allow		IPv6	UDP	WAN3 (WAN)		fe80::/10		fe80	≡ ⊠ ⊡	
	WAN2_Allow		IPv6	ICMP	WAN3 (WAN)		fe80::/10	-	~	≐ ₪ ⊡	
	WAN2_Allow-I		IPv6	ICMP	WAN3 (WAN)		-			≑ ⊠ ⊡	

Traffic Rules list