

How to define Content Blocking on RS series gateway to allow accessing few website only

1. Policy Object → Content Blocking → URL

If user want to block all website and allow accessing few website, user can add “~” sign before the website domain name, it means this website is allowed to be accessed.

Add New URL String

URL String

(Max. 30 characters)

↓

Add New URL String

URL String

(Max. 30 characters)

↓

URL String	Configure
~www.airlive.com	<div>ModifyRemove</div>
~www.airlive.latin.com	<div>ModifyRemove</div>

2. Create third Content Blocking rule to block all website. “*” sign indicates “all”.

Add New URL String

URL String

(Max. 30 characters)

↓


URL String	Configure
~www.airlive.com	<div>ModifyRemove</div>
~www.airlive.latin.com	<div>ModifyRemove</div>
*	<div>ModifyRemove</div>

3. Policy → Outgoing Policy

Enable Content Blocking on Outgoing Policy setting, so LAN user can only access the websites www.airlive.com and www.airlive.latin.com.

Add New Policy	
Source Address	Inside_Any ▾
Destination Address	Outside_Any ▾
Service	ANY ▾
Schedule	None ▾
Authentication User	None ▾
Tunnel	None ▾
Action, WAN Port	PERMIT ALL ▾
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input checked="" type="checkbox"/> Enable
IM / P2P Blocking	None ▾
QoS	None ▾
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps (0: means unlimited)
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> (Range: 1 - 99999, 0: means unlimited)
MAX. Concurrent Sessions	<input type="text" value="0"/> (Range: 1 - 99999, 0: means unlimited)



4. If only few users need to be restricted to access specific website, you can define those user's IP address on **Policy Object → Address → LAN** first, and group those users as a group, and enable it on Outgoing Policy.

 Policy Object > Address > LAN

Name	IP / Netmask	MAC Address	Configure
Inside_Any	0.0.0.0/0.0.0.0		<input type="button" value="In Use"/>
Jacky	192.168.1.10/255.255.255.255		<input type="button" value="Modify"/> <input type="button" value="Remove"/>
Portia	192.168.1.200/255.255.255.255		<input type="button" value="Modify"/> <input type="button" value="Remove"/>
Eva	192.168.1.101/255.255.255.255		<input type="button" value="Modify"/> <input type="button" value="Remove"/>

- System
- Interface
- Policy Object
 - Address
 - LAN
 - LAN Group
 - WAN
 - WAN Group
 - DMZ
 - DMZ Group
 - Service




Policy Object > Address > LAN Group


- System
- Interface
- Policy Object
- Address
 - LAN
 - LAN Group
 - WAN
 - WAN Group
 - DMZ
 - DMZ Group
- Service
- Schedule
- QoS
- Authentication
- Content Blocking
- IM / P2P Blocking
- Virtual Server
- VPN
- Policy

Add New Address Group

Name: (Max. 16 characters)

<--- Available address --->

Jacky
Portia
Eva

Add ➡

⬅ Remove


<--- Selected address --->






Jacky
Portia
Eva



Modify Policy

Source Address	Web_restrict ▼
Destination Address	Outside_Any ▼
Service	ANY ▼
Schedule	None ▼
Authentication User	None ▼
Tunnel	None ▼
Action, WAN Port	PERMIT ALL ▼
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input checked="" type="checkbox"/> Enable
IM / P2P Blocking	None ▼
QoS	None ▼
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps (0: means unlimited)
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> (Range: 1 - 99999, 0: means unlimited)
MAX. Concurrent Sessions	<input type="text" value="0"/> (Range: 1 - 99999, 0: means unlimited)

- 
Policy > Outgoing

- System
 - Interface
 - Policy Object
 - Policy
 - Outgoing
 - Incoming
 - WAN To DMZ
 - LAN To DMZ
 - DMZ To WAN
 - DMZ To LAN
 - Anomaly Flow IP
 - Monitor

Source	Destination	Service	Action	Option				Configure			Move
Web_restrict	Outside_Any	ANY						Modify	Remove	Pause	To 1
Inside_Any	Outside_Any	ANY						Modify	Remove	Pause	To 2

New Entry

Source	Destination	Service	Action	Option				Configure			Move
Web_restrict	Outside_Any	ANY									To 1 
Inside_Any	Outside_Any	ANY									To 2 