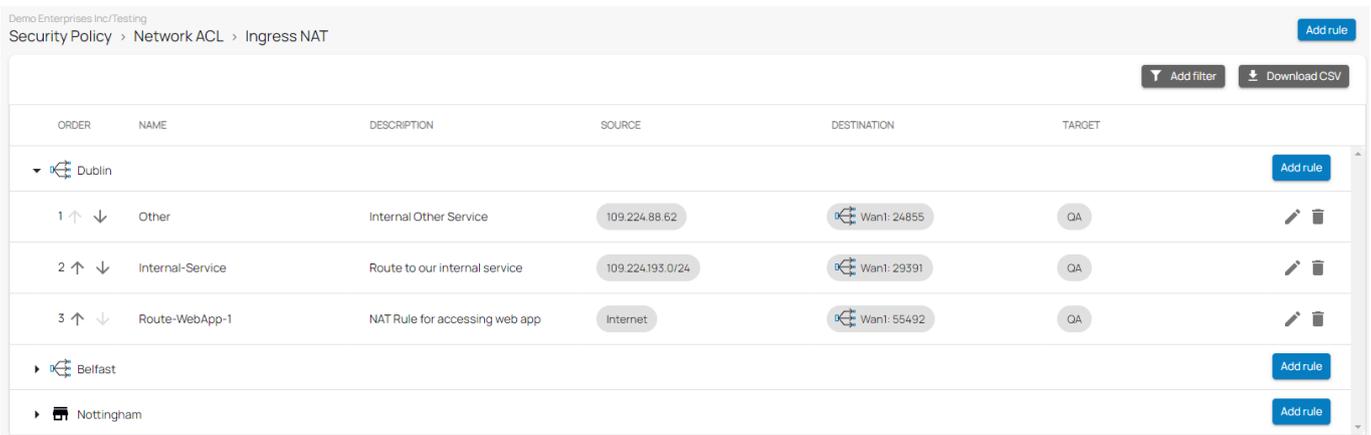


## How to Create Ingress NAT Rules

<https://campus.barracuda.com/doc/98223645/>

The Barracuda SecureEdge allows administrators to create ingress NAT rules for sites and on-premise gateways. Ingress traffic means any form of network traffic and data communication from external networks to destinations inside the host network. In the network policies, you can add a new ingress NAT rule by specifying source, destination, and target criteria, edit an existing ingress NAT rule, and remove an existing ingress NAT rule.



The screenshot shows the 'Ingress NAT' configuration page for the 'Dublin' site. The page has a breadcrumb trail: 'Security Policy > Network ACL > Ingress NAT'. There are buttons for 'Add rule', 'Add filter', and 'Download CSV'. The main table lists three NAT rules:

ORDER	NAME	DESCRIPTION	SOURCE	DESTINATION	TARGET	
1	Other	Internal Other Service	109.224.88.62	Wan1: 24855	QA	[Edit] [Delete]
2	Internal-Service	Route to our internal service	109.224.193.0/24	Wan1: 29391	QA	[Edit] [Delete]
3	Route-WebApp-1	NAT Rule for accessing web app	Internet	Wan1: 55492	QA	[Edit] [Delete]

Below the table, there are expandable sections for 'Belfast' and 'Nottingham', each with an 'Add rule' button.

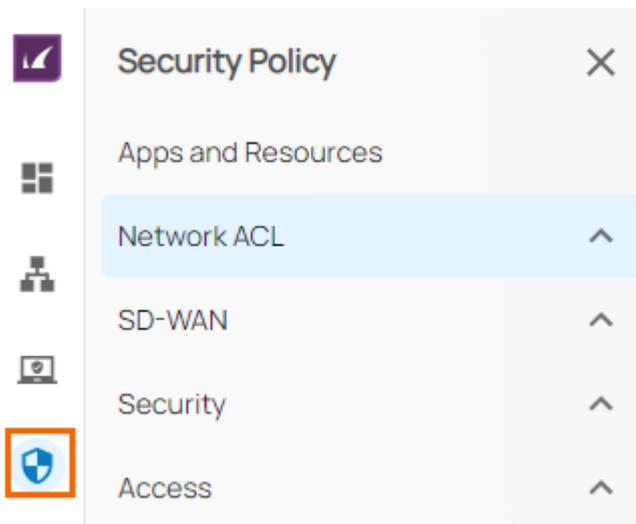
## Requirements and Limitations

- For information on the limitation of DNS objects (512 per default), see [Hostname \(DNS Resolvable\) Network Objects](#) in the CloudGen Firewall documentation.
- To enable a security feature against ingress traffic, you must use the same application as target of the ingress rule and as destination of the security feature. Do not use local firewall IPs as redirect targets.
- HA session sync does not work for ingress traffic coming through dynamic ISPs (DHCP).

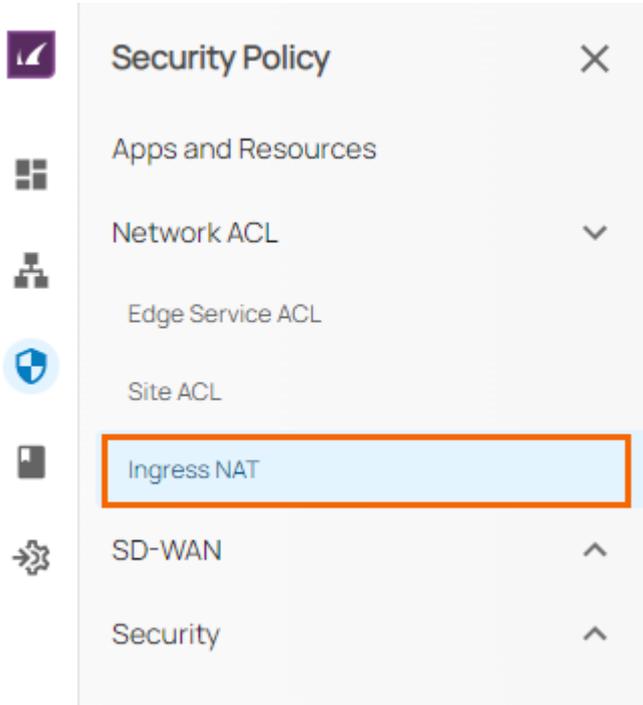
SD-WAN policies and SSL inspection are not supported for ingress traffic.

## Create an Ingress NAT Rule

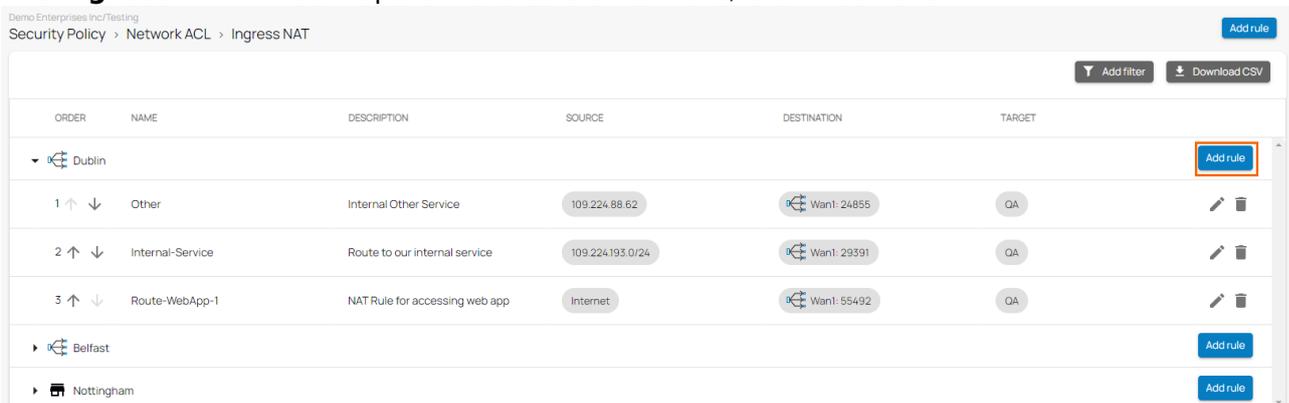
1. Go to <https://se.barracudanetworks.com> and log in with your existing Barracuda Cloud Control account.
2. Select the workspace containing your site.
3. In the left menu, click the **Security Policy** icon.



4. Expand the **Network ACL** menu and select the **Ingress NAT**.



5. The **Ingress NAT** window opens. To create a new rule, click **Add rule**.



6. In the **Add New Rule** window, specify values for the following:

- **Name** - Enter a name.
- **Description** - Enter a description.
- In the **SOURCE CRITERIA** section, specify the following:
  - **Type** - Select a source type. You can choose between **Internet** and **IP/Network**.
  - When selecting **IP/Network**, enter the IP address or network, and click **+**.
- In the **DESTINATION CRITERIA** section, specify the following:
  - **Type** - Select a destination type. You can choose between **Private Edge** and **Site**.
  - **Private Edge** - Select your destination private edge.
  - **WAN** - Select your destination WAN interface according to the public IP you need.  
Note: In addition, you can also add PPPoE WAN interfaces.
  - **PAT Public Port** - Select the destination PAT public port.
- In the **TARGET CRITERIA** section, the target is defined as a custom application.
  - **Application/Resources** - Select an application.

### Add New Rule ✕

**i** Name \*

**i** Description

SOURCE CRITERIA

**i** Type \*

**i** IP/Network \*

DESTINATION CRITERIA

**i** Type \*

**i** Private Edge \*

**i** WAN \*

**i** PAT Public Port

TARGET CRITERIA

**i** Application/Resource \*

7. Click **Save**.

## Edit an Existing Ingress NAT Rule

To edit an existing ingress NAT rule:

1. Expand the **Network ACL** menu on the left and select the **Ingress NAT**. The **Ingress NAT** window opens.

- Click on the pencil icon next to the rule you want to edit.

Demo Enterprises Inc/Testing  
Security Policy > Network ACL > Ingress NAT

Add rule

Add filter Download CSV

ORDER	NAME	DESCRIPTION	SOURCE	DESTINATION	TARGET	
<div style="display: flex; justify-content: space-between; align-items: center;"> <span>▼ Dublin</span> <span>Add rule</span> </div>						
1	Other	Internal Other Service	109.224.88.62	Wan1: 24855	QA	 
2	Internal-Service	Route to our internal service	109.224.193.0/24	Wan1: 29391	QA	 
3	Route-WebApp-1	NAT Rule for accessing web app	Internet	Wan1: 55492	QA	 
<div style="display: flex; justify-content: space-between; align-items: center;"> <span>▶ Belfast</span> <span>Add rule</span> </div>						
<div style="display: flex; justify-content: space-between; align-items: center;"> <span>▶ Nottingham</span> <span>Add rule</span> </div>						

- The **Edit Rule** window opens. Edit the value you are interested in.
- Click **Save**.

## Remove an Existing Ingress NAT Rule

To remove an existing ingress NAT rule:

- Expand the **Network ACL** menu on the left and select **Ingress NAT**. The **Ingress NAT** window opens.
- Click on the trash can icon next to the rule you want to remove.

Demo Enterprises Inc/Testing  
Security Policy > Network ACL > Ingress NAT

Add rule

Add filter Download CSV

ORDER	NAME	DESCRIPTION	SOURCE	DESTINATION	TARGET	
<div style="display: flex; justify-content: space-between; align-items: center;"> <span>▼ Dublin</span> <span>Add rule</span> </div>						
1	Other	Internal Other Service	109.224.88.62	Wan1: 24855	QA	 
2	Internal-Service	Route to our internal service	109.224.193.0/24	Wan1: 29391	QA	 
3	Route-WebApp-1	NAT Rule for accessing web app	Internet	Wan1: 55492	QA	 

- The **Delete Rule** window opens.

Delete Rule

Are you sure you want to delete this rule?

Cancel

Ok

- Click **OK** to confirm.

## Filtering Functions

You can add filters to view specific content on the page. Click **Add Filter** in the top-right corner of a page and select the criteria you wish to search for.



To reset the filter, click **Clear Filters**.

## Figures

1. Add-NAT- rule.png
2. goto-secpolicy.png
3. goto-secpolicy-ingressNAT.png
4. goto-Add-rule.png
5. ingress\_nat\_add\_rule.png
6. edit-NAT- rule.png
7. remove-nat-rule.png
8. delete\_rule\_ingress.png
9. add\_filter.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.