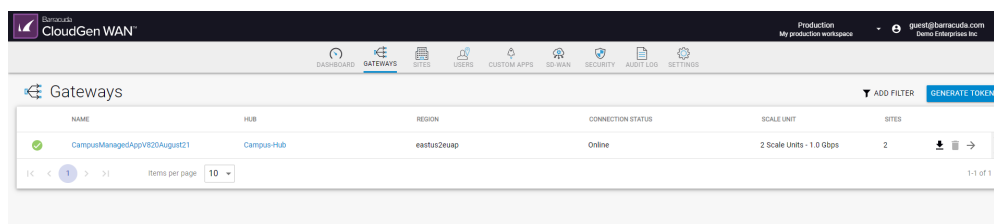


Gateway ACL

<https://campus.barracuda.com/doc/95264095/>

With access control lists, you can either allow or deny access based on source and destination. You can use either the predefined applications or a custom application. For more information on custom applications, see [Policies](#) and [How to Create Custom Applications](#) .



Before You Begin

- If you want to select users or groups in the policies, you must first connect your Azure Active Directory. For more information, see [How to Connect Your Azure Active Directory with Barracuda Cloud Control](#).

Create an ACL

1. Open <https://cloudgenwan.barracudanetworks.com/> and log in with your existing Barracuda Cloud Control account.
2. Go to **SECURITY > GATEWAY ACL**.
3. To create a new rule, click **ADD RULE** .
4. The **Add New Rule** window opens.
 - Specify values for the following:
 - **Scope** – Select the scope of this rule from the drop-down menu.
 - **Name** – Enter a name.
 - **Description** – Enter a description.
 - **Action** – Specify the action.
 - In the **SOURCE CRITERIA** section:
 - **Type** – Select a source type. You can choose between **Custom Network Application**, **IP/Network**, **Site**, **User/Group**, and **User Connectivity (VPN)**. If you want to select users or groups in the policies, you must first connect your Azure Active Directory. For more information, see [How to Connect Your Azure Active Directory with Barracuda Cloud Control](#).
 - **IP/Network** – Enter the IP address or network, and click +.
 - In the **DESTINATION CRITERIA** section:

- **Type** – Select a destination type. You can choose between **IP/Network** , **Site** , **User/Group** , and **User Connectivity (VPN)** .
- **Application** – Select an application.

Add New Rule ×

i Scope *

All Gateways × ▼

i Name *

GW-ACL

i Description

AllowFTP

i Action *

✓ Allow ▼

SOURCE CRITERIA

Type *

IP/Network ▼

IP/Network *

10.17.94.0/24 ×

+

DESTINATION CRITERIA

Type *

Application ▼

Application *

⚙ FTP ×

Type to search ▼

CANCEL

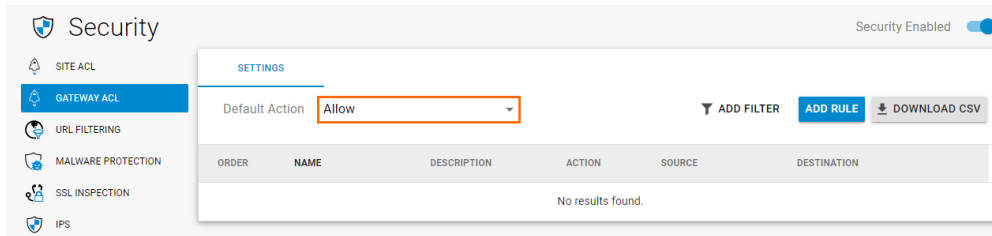
SAVE

5. Click **SAVE**.

Select the Default Action

You can configure the Site ACL to either block or allow traffic by default.

1. Open <https://cloudgenwan.barracudanetworks.com/> and log in with your existing Barracuda Cloud Control account.
2. Go to **SECURITY > GATEWAY ACL**.
3. In the **SETTINGS** section select the default action.



Further Information

- For more information on User and Groups, see [How to Connect Your Azure Active Directory with Barracuda Cloud Control](#).
- For more information on User Connectivity, see [User Connectivity & Personal Security](#).

Figures

1. gw821_depl.png
2. gw_rule82.png
3. gw_default_Action.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.