How to Create a Site ACL

https://campus.barracuda.com/doc/100368791/

The Barracuda SecureEdge Manager allows you to create access control lists (ACLs) for your connected sites, using either predefined applications or a custom application. With access control lists, you can either allow or deny access based on source and destination.

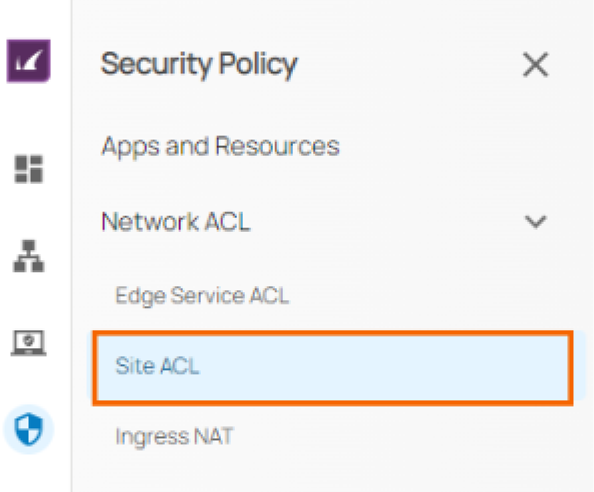
> Note that ICMP via the Barracuda SecureEdge Agent is always set to allow for configured ZTNA resources. For example, you can ping an internal resource via SecureEdge Agent if a policy for it exists. For more information on SecureEdge Access, see SecureEdge Access.

Before You Begin

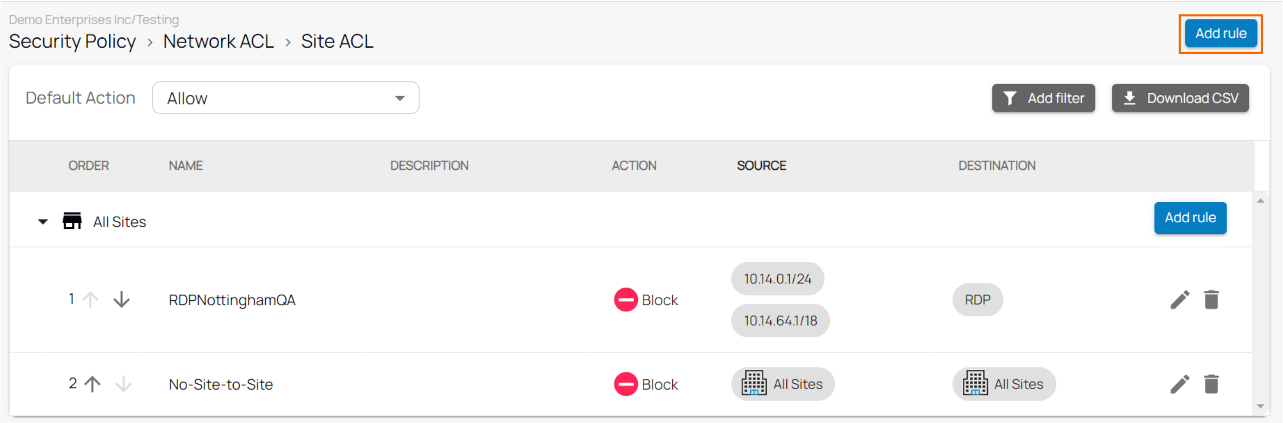
- To select users or groups in the policies, you must first connect your Microsoft Entra ID . For more information, see How to Connect Your Microsoft Entra ID with Barracuda Cloud Control.

Create a Site ACL

1. Go to https://se.barracudanetworks.com and log in with your existing Barracuda Cloud Control account.
2. In the left menu, click the **Tenants/Workspaces** icon and select the workspace containing your site.
3. Go to **Security Policy**.
4. Expand the **Network ACL** menu on the left and select **Site ACL**.



5. The **Site ACL** window opens. To create a new rule, click **Add Rule**.

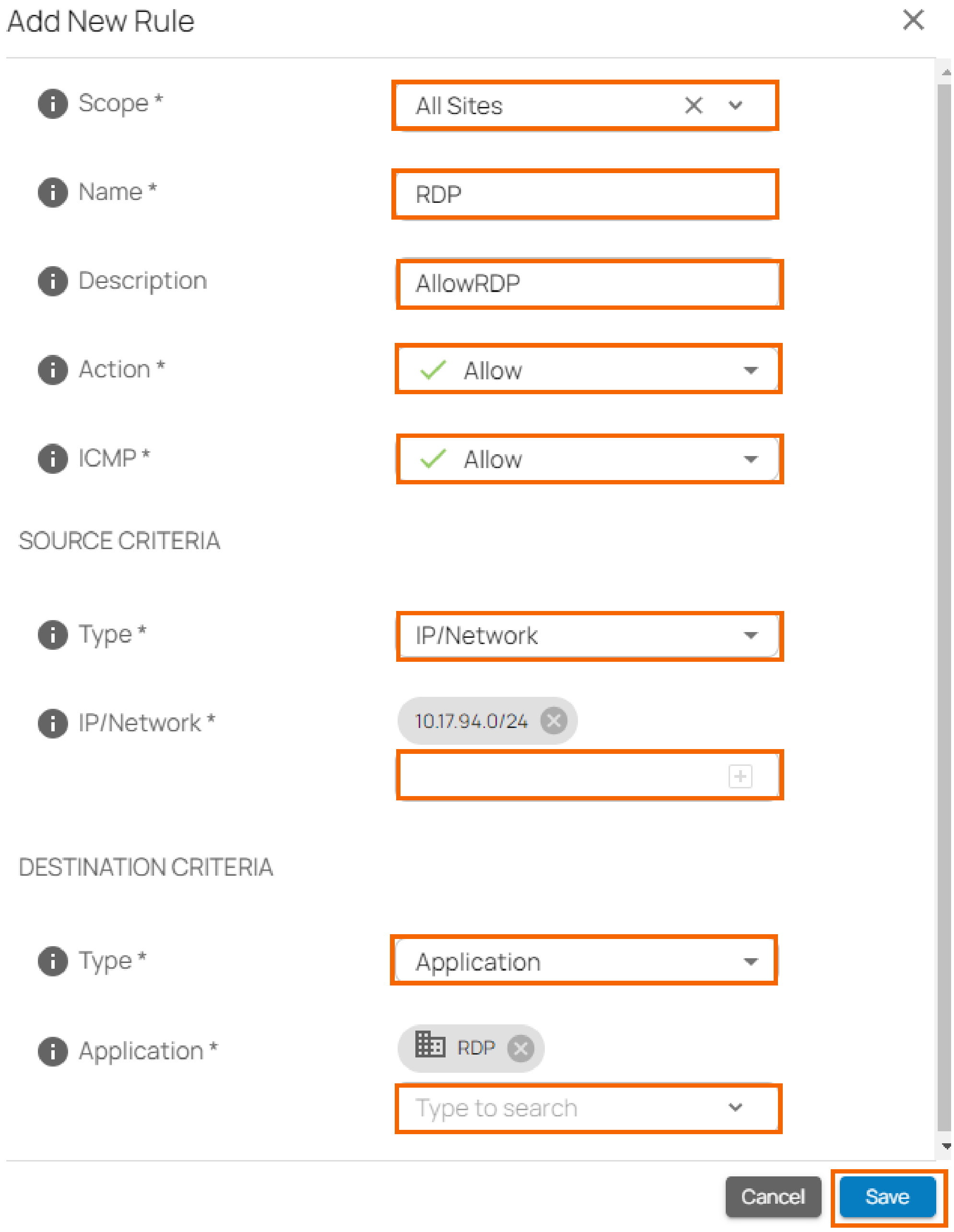


Demo Enterprises Inc/Testing

Security Policy › Network ACL › Site ACL

ORDER	NAME	DESCRIPTION	ACTION	SOURCE	DESTINATION
All Sites					
1	RDPNottinghamQA		Block	10.14.0.1/24 10.14.64.1/18	RDP
2	No-Site-to-Site		Block	All Sites	All Sites

6. 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 unique name for a rule.
    - **Description** – Enter a brief description.
    - **Action** – Select the action from the drop-down menu. You can choose between **Allow** and **Block.**
    - **ICMP** – Select the ICMP value from the drop-down menu. You can choose between **Allow** and **Block**.
        - If you select **Action = Allow**, you can choose an ICMP value of either **Allow** or **Block**.
        - If you select **Action = Block**, the ICMP field is disabled and set to **Block**.
    - In the **SOURCE CRITERIA** section, specify the following:
        - **Type** – Select a source type. You can choose between **IP/Network**, **Private Edge Service**, **Site**, **User/Group**, and **User Connectivity (VPN)**. To select users or groups in the policies, you must first connect your Microsoft Entra ID . For more information, see How to Connect Your Microsoft Entra ID with Barracuda Cloud Control.
            - **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 **Application**, **IP/Network**, **Site**, **User Connectivity (VPN),** and **Private Edge Service**.
        - **Application** – Select an application from the drop-down menu, or type to search.



Add New Rule

Scope * All Sites

Name * RDP

Description AllowRDP

Action * ✓ Allow

ICMP * ✓ Allow

SOURCE CRITERIA

Type * IP/Network

IP/Network * 10.17.94.0/24

DESTINATION CRITERIA

Type * Application

Application * RDP

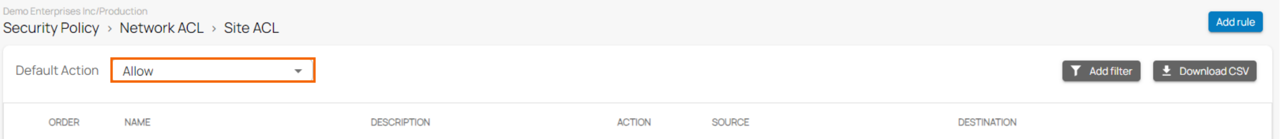
7. Click **Save**.

After the configuration is complete, you can either allow or deny access based on source and destination. For example, when the **Action** and **ICMP** fields are set to **Allow**, you can send a ping from the source to the destination. If no Site ACL rule matches, the **Default Action** will be applied.

Select the Default Action

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

1. Go to https://se.barracudanetworks.com and log in with your existing Barracuda Cloud Control account.
2. In the left menu, click the **Tenants/Workspaces** icon and select the workspace containing your site.
3. Go to **Security Policy**.
4. Expand the **Network ACL** menu on the left and select **Site ACL**.
5. The **Site ACL** page opens. Select the **Default Action**.



Demo Enterprises Inc/Production

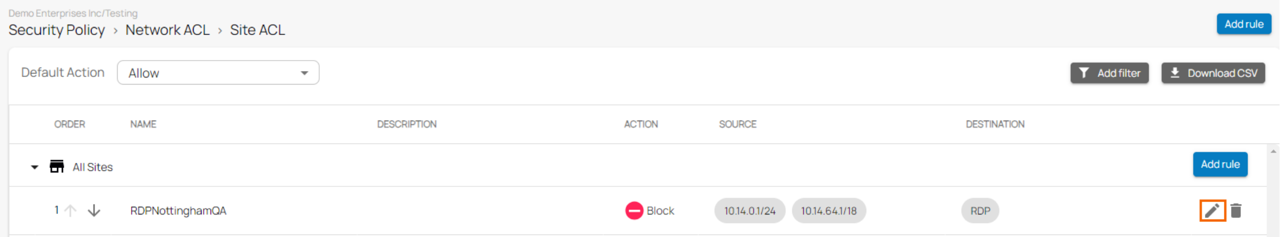
Security Policy › Network ACL › Site ACL

Default Action: Allow

ORDER	NAME	DESCRIPTION	ACTION	SOURCE	DESTINATION

Edit an Existing Site ACL

1. In the left menu, click the **Security Policy**.
2. Expand the **Network ACL** menu on the left and select **Site ACL**.
3. The **Site ACL** window opens. Click on the pencil icon next to the rule you want to edit.



Demo Enterprises Inc/Testing

Security Policy › Network ACL › Site ACL

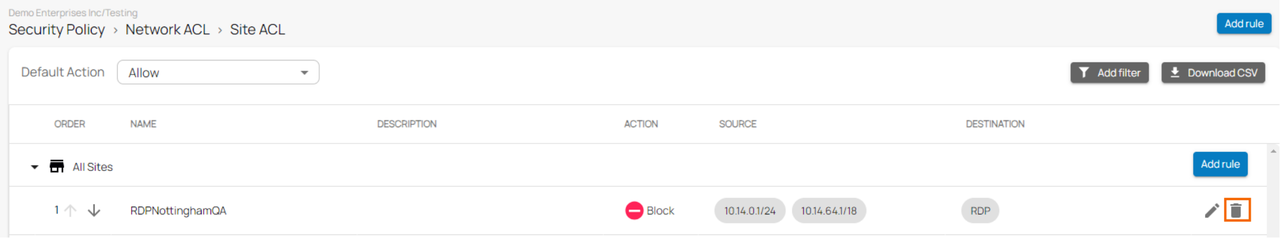
Default Action: Allow

ORDER	NAME	DESCRIPTION	ACTION	SOURCE	DESTINATION
All Sites					
1	RDPNottinghamQA		Block	10.14.0.1/24 10.14.64.1/18	RDP

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

Remove an Existing Site ACL

1. In the left menu, click the **Security Policy**.
2. Expand the **Network ACL** menu on the left and select **Site ACL**.
3. The **Site ACL** window opens. Click on the trash can icon next to the rule you want to remove.



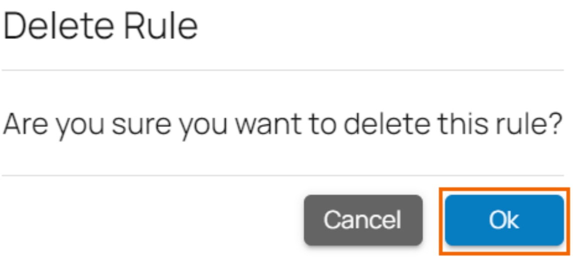
Demo Enterprises Inc/Testing

Security Policy › Network ACL › Site ACL

Default Action: Allow

ORDER	NAME	DESCRIPTION	ACTION	SOURCE	DESTINATION
All Sites					
1	RDPNottinghamQA		Block	10.14.0.1/24 10.14.64.1/18	RDP

4. The **Delete Rule** window opens.



Delete Rule

Are you sure you want to delete this rule?

5. Click **OK** to confirm.

Further Information

- For more information on Edge Service ACL, see How to Create an Edge Service ACL.
- For more information on User Connectivity, see Point-to-Site.

Figures