# Example - Allowing Access to the Internet

https://campus.barracuda.com/doc/8650764/

When you configure access rules to allow network traffic, you can choose to allow traffic only for certain types of traffic that are passing to and from specific networks. You might want to create rules that allow wanted traffic to pass, and then use the BLOCKALL rule to block all other types of traffic.

This article provides an example of how to configure a access rule that only allows HTTP and HTTPS connections from the local 192.168.200.0/24 network to the Internet.

## Video

Watch the video below to see an example of an ALLOW access rule configured on the Barracuda NextGen Firewall X-Series.


## Step 1. Create the Access Rule to Allow Traffic to the Internet

1. Go to the **FIREWALL > Firewall Rules** page.
2. Click **Add Access Rule** to create a new access rule.
3. In the **Add Access Rule** window, enter a name and description for the rule.
4. Specify the following settings:

| Action | Connection | Service | Source | Destination |
|---|---|---|---|---|
| Allow | Default (SNAT) | Any | Trusted LAN | Internet |

To allow connections from the local network to the Internet, the X-Series Firewall must perform source-based NAT. The source IP address of outgoing packets is changed from that of the client residing in the LAN to the WAN IP address of the X-Series Firewall, so the connection is established between the WAN IP address and destination IP address. The destination address of

reply packets belonging to this session is rewritten with the client's IP address.

5. Click **Save**.

### Step 2. Verify the Order of the Access Rules

New rules are created at the bottom of the firewall rule set. Rules are processed from top to bottom in the rule set. Drag your access rule to a slot in the rule list, so that no access rules before it matches this traffic. Verify that your rules are placed above the BLOCKALL rule. Otherwise, the rule never matches.

After adjusting the order of rules in the rule set, click **Save**.