Example - Creating Time-Based Access Rules

https://campus.barracuda.com/doc/8650763/

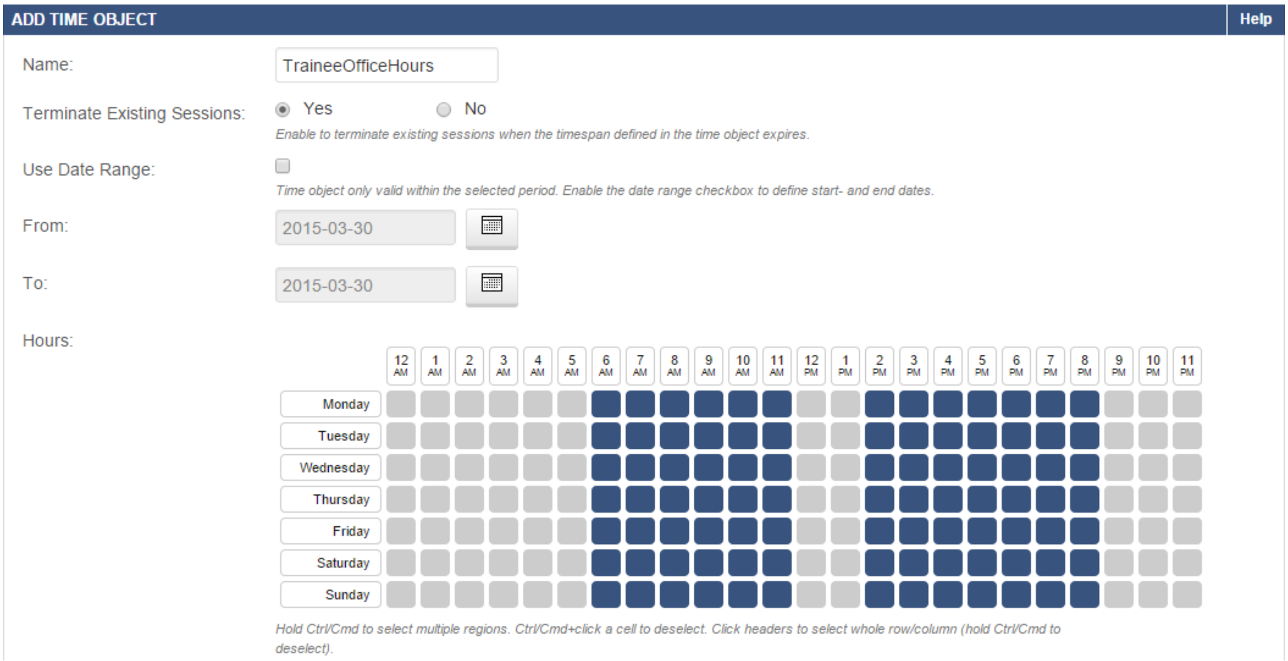
With the Barracuda NextGen Firewall X-Series, you can configure access rules that are only active for specific times or dates. Create a time object for the times that the access rule should be active. Then apply this time object to the access rule.

This article provides an example of how to configure a access rule that blocks Internet (HTTP and HTTPS) access for two trainees from Monday to Friday, except during the hours of 11:00 AM to 01:00 PM. The two trainees reside in the 192.168.200.0/24 network segment and use computers with the 192.168.200.100 and 192.168.200.101 IP addresses.

Step 1. Create a Time Object

This example configures a time object named **TraineeOfficeHours** that includes all office hours except lunch time from **12am** to **1pm**.

1. Go to the **FIREWALL > Time Objects** page.
2. In the **Time Objects** section, click **Add Time Object**.
3. In the **Name** field, enter `TraineeOfficeHours`.
4. To terminate existing sessions when the access rule is applied, set **Terminate Existing Sessions** to **Yes**.
5. To define a date range for this time object, select the **Use Date Range** check box.
6. In the time table of the configuration window, select all days and times when the access rule should be active.



Name: TraineeOfficeHours

Terminate Existing Sessions: ● Yes ○ No

Enable to terminate existing sessions when the timespan defined in the time object expires.

Use Date Range: □

Time object only valid within the selected period. Enable the date range checkbox to define start- and end dates.

From: 2015-03-30

To: 2015-03-30

Hours:

	12 AM	1 AM	2 AM	3 AM	4 AM	5 AM	6 AM	7 AM	8 AM	9 AM	10 AM	11 AM	12 PM	1 PM	2 PM	3 PM	4 PM	5 PM	6 PM	7 PM	8 PM	9 PM	10 PM	11 PM
Monday	□	□	□	□	□	□	■	■	■	■	■	■	□	□	■	■	■	■	■	■	■	□	□	□
Tuesday	□	□	□	□	□	□	■	■	■	■	■	■	□	□	■	■	■	■	■	■	■	□	□	□
Wednesday	□	□	□	□	□	□	■	■	■	■	■	■	□	□	■	■	■	■	■	■	■	□	□	□
Thursday	□	□	□	□	□	□	■	■	■	■	■	■	□	□	■	■	■	■	■	■	■	□	□	□
Friday	□	□	□	□	□	□	■	■	■	■	■	■	□	□	■	■	■	■	■	■	■	□	□	□
Saturday	□	□	□	□	□	□	■	■	■	■	■	■	□	□	■	■	■	■	■	■	■	□	□	□
Sunday	□	□	□	□	□	□	■	■	■	■	■	■	□	□	■	■	■	■	■	■	■	□	□	□

Hold Ctrl/Cmd to select multiple regions. Ctrl/Cmd+click a cell to deselect. Click headers to select whole row/column (hold Ctrl/Cmd to deselect).

7. Click **Add** to create the time object.

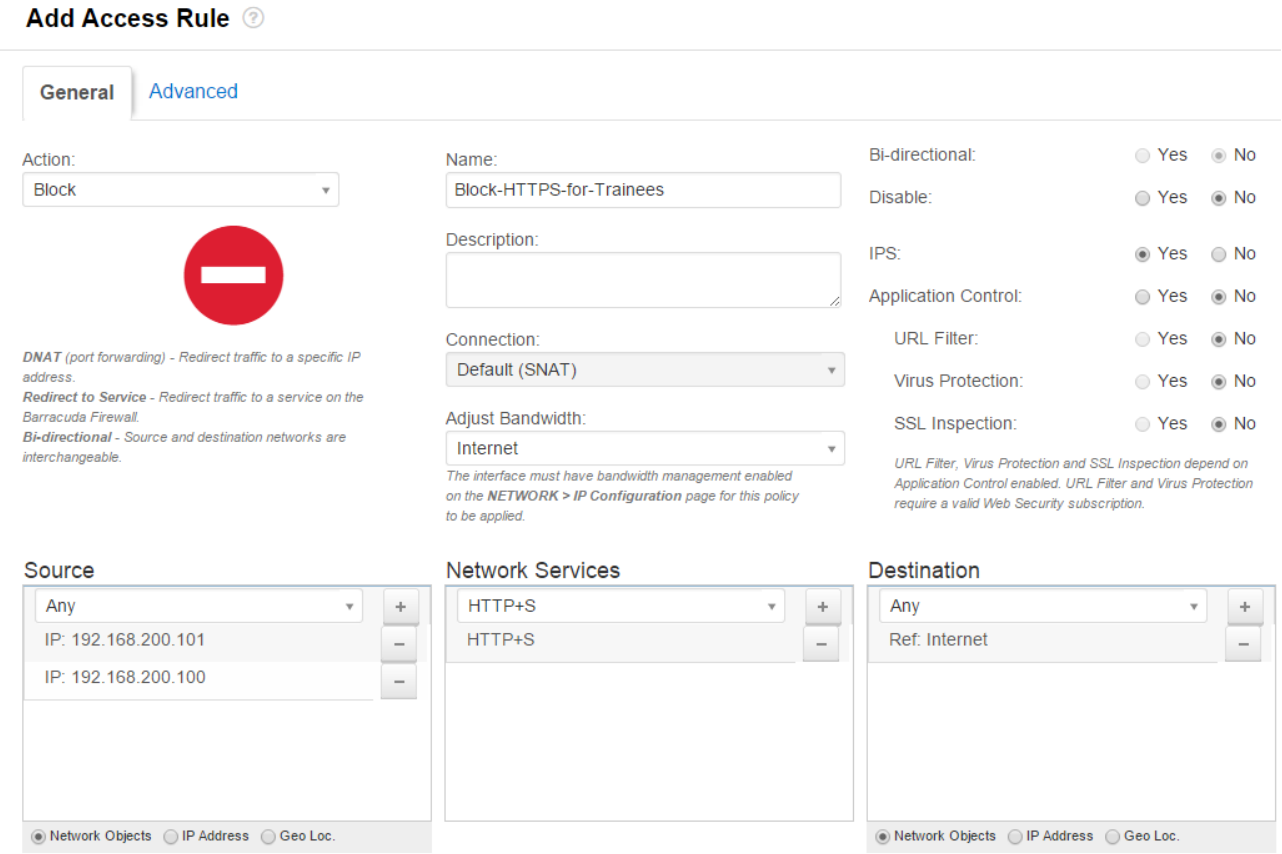
Step 2. Create an Access Rule using the Time Object

This example configures an access rule named Block-HTTPs-for-Trainees that blocks HTTP and HTTPS network traffic from the 192.168.200.100 and 192.168.200.101 IP addresses.

1. Go to the **FIREWALL > access rules** page.
2. Click **Add Access Rule** to create a new access rule. The **Add Access Rule** window opens.
3. Enter a name and description for the rule.
4. Specify the following settings:

Name	Action	Connection	Service	Source	Destination
`Block-HTTPS-for-Trainees`	**Block**	**Default (SNAT)**	**HTTP+S**	∘ `192.168.200.100` ∘ `192.168.200.101`	**Internet**

Because all other clients in the 192.168.200.0/24 network should not be affected by this rule, the source network is limited to the 192.168.200.100 and 192.168.200.101 IP addresses.



Add Access Rule

General | Advanced

Action: Block

DNAT (port forwarding) - Redirect traffic to a specific IP address.
Redirect to Service - Redirect traffic to a service on the Barracuda Firewall.
Bi-directional - Source and destination networks are interchangeable.

Name: Block-HTTPS-for-Trainees

Description:

Connection: Default (SNAT)

Adjust Bandwidth: Internet

The interface must have bandwidth management enabled on the NETWORK > IP Configuration page for this policy to be applied.

Bi-directional: ○ Yes ● No

Disable: ○ Yes ● No

IPS: ● Yes ○ No

Application Control: ○ Yes ● No

URL Filter: ○ Yes ● No

Virus Protection: ○ Yes ● No

SSL Inspection: ○ Yes ● No

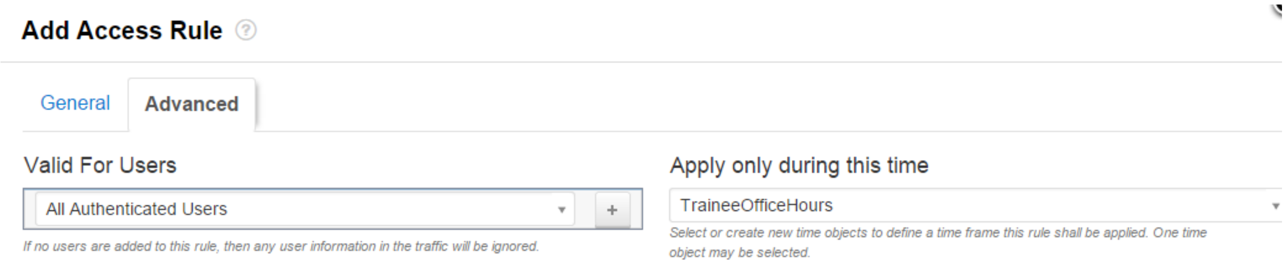
URL Filter, Virus Protection and SSL Inspection depend on Application Control enabled. URL Filter and Virus Protection require a valid Web Security subscription.

Source: Any
IP: 192.168.200.101
IP: 192.168.200.100
● Network Objects ○ IP Address ○ Geo Loc.

Network Services: HTTP+S
HTTP+S

Destination: Any
Ref: Internet
● Network Objects ○ IP Address ○ Geo Loc.

5. Click the **ADVANCED** tab.
6. From the **APPLY ONLY DURING THIS TIME** list, select the time object that you created. For this example, select the **TraineeOfficeHours** object.



Add Access Rule

Valid For Users: All Authenticated Users

If no users are added to this rule, then any user information in the traffic will be ignored.

Apply only during this time: TraineeOfficeHours

Select or create new time objects to define a time frame this rule shall be applied. One time object may be selected.

7. At the top of the window, click **Save**.

Step 3. Verify the Order of the Access Rules

Access rules are processed from top to bottom. Place your access rule before any other access rule that matches the same traffic. For this example, place your time-based block rule before any rule that allows Internet access. Click **Save** to save the changes to the order of the access rules.

Figures

1. time_object1_67_01.png
2. time_object1_67_02.png
3. time_object1_67_03.png