How to Create an Application Rule

https://campus.barracuda.com/doc/41115758/

Configuring an application rule is similar to configuring a forwarding firewall rule. However, you must first enable application control in the forwarding firewall rule that it will apply to. You must also specify if you want to use SSL interception. The following example shows how to create an application rule to prevent users from accessing a social networking application from the LAN.

In this article:

Before you Begin

Verify that you have enabled Application Control 2.0. If you are using SSL Inspection, also verify that you have enabled and configured it. For more information, see How to Enable Application Control 2.0, SSL Interception, URL Filtering, Virus Scanning and ATP.

Step 1. Enable Application Control in the Forwarding Firewall Rule

1. Open the **Forwarding Rules** page (**Config > Full Config > Virtual Servers > *your virtual server* > Assigned Services > Firewall**).
2. **Edit** the firewall rule you want to enable application control for.
3. In the **Policy** section, select a policy from the **Application Policy** list to enable application control. You can also enable SSL interception. Select one of the following options:

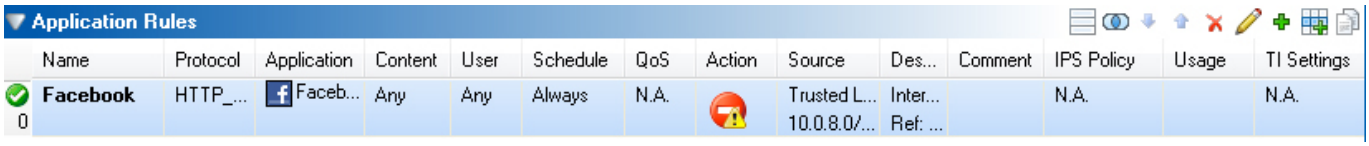
Option	Description
App Control + SSL Interception + URL Filter + AV Scanning + ATD	Enables application rules with SSL interception, URL filtering and AV scanning with Advanced Threat Protection.
App Control + SSL Interception + URL Filter + AV Scanning	Enables application rules with SSL interception, URL filtering and AV scanning.
App Control + SSL Interception + URL Filter	Enables application rules with SSL interception and URL filtering.
App Control + URL Filter	Enables application rules and URL Filter.
App Control + SSL Interception	Enables application rules and SSL interception.
App Control	Only enables application rules.
No App Control	Disables application control for this firewall rule.

4. Click **OK**.

5. Click **Send Changes** and **Activate**.

Step 2. Create an Application Rule

1. Open the **Forwarding Firewall Rules** page.
2. From the **Rule Lists** menu, select **Application Rules**.
3. Click **Lock**.
4. Add the rule by either clicking the green plus sign (**+**) in the top right of the page or right-clicking the rule set and selecting **New > Rule**.
5. From the rule set, select the **New Rule** (under the **Name** column).
6. Edit the new rule by either clicking the pen icon in the top right or right-clicking the rule and selecting **Edit Rule**.
7. Enter a name for the rule. For example, enter *Facebook* if you are creating an application rule for Facebook.



In the **Protocol** field, you can specify the protocols to which the rule should apply. For example, **HTTP_direct**.

If you allow a protocol in an application rule, the protocol must also be allowed by the forwarding firewall rule affecting network traffic from the same source to the same destination. If the forwarding firewall rule denies a protocol, the protocol is automatically denied for the use of application rules.

Step 3. Configure the Application Rule

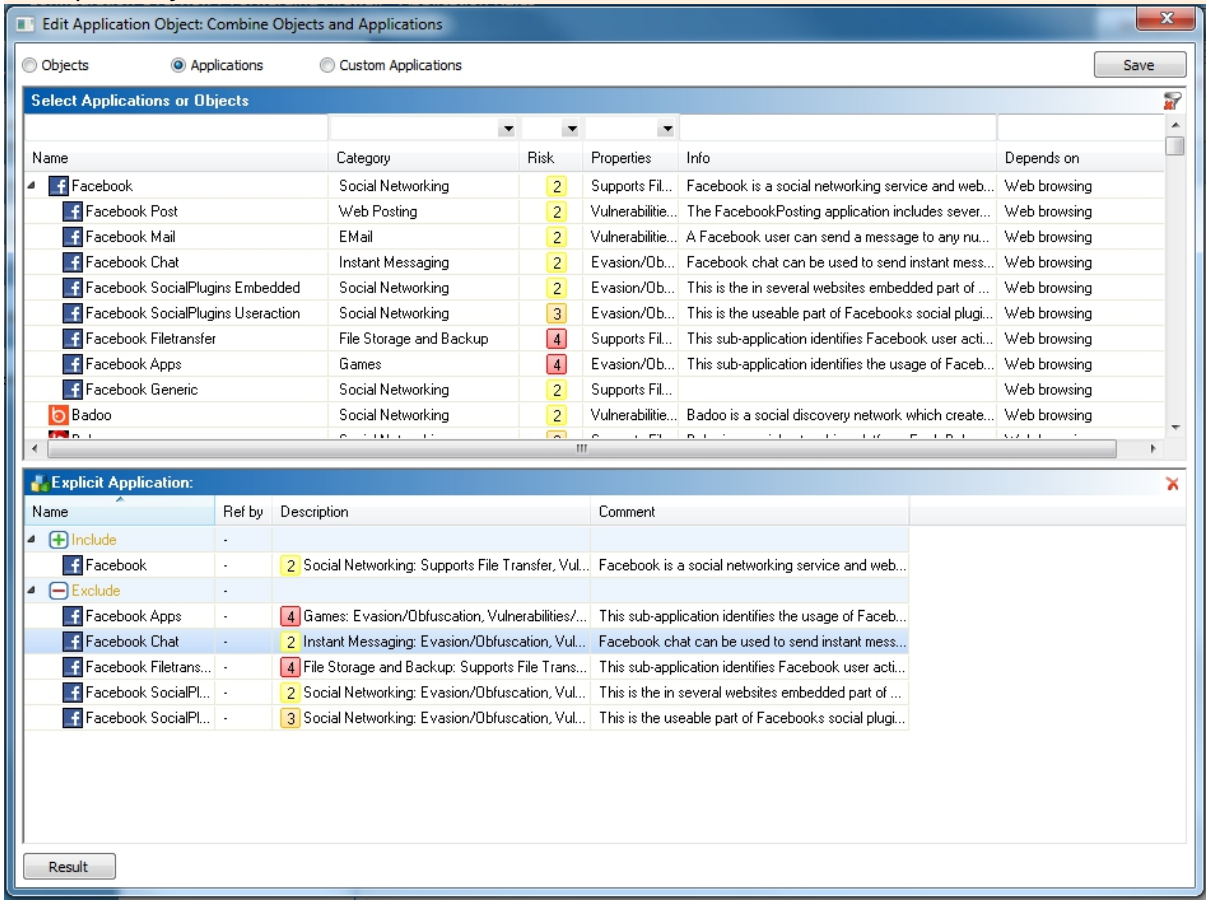
To configure the application rule:

1. Open the application rule configuration.
2. Select the **Application** field, click the **pen** icon, and select **<Create Explicit Application>**.
3. To filter the applications, enter the application name in the field on top of the list (you can also press **Ctrl**+**F**). You can also filter the list by selecting criteria from the filter lists.
4. To add an application:
    1. In the **Edit Application window**, click **Applications**.
    2. Select the application from the list.
    3. Click the plus sign (**+**) next to the application name.The application is then displayed in the **Explicit Application** list.
5. If the application consists of more than one component, you can exclude specific components

from it. To exclude a component:

1. Expand the application in the **Select Applications or Objects** list.
2. Click the minus sign (**-**) next to the application features that you want to exclude.

   The *base* component belongs to the application and must never be excluded separately.



6. Click **Save**.
7. Specify the remaining settings:
   1. In the **User** field, select **<Create Explicit User>**, click **New** in the upcoming window, and specify the details. Then click **OK** to return to the rule configuration.
   2. With the **Schedule** parameter, you can specify a time frame for the rule.
   3. In the **Action** field, select an action for the rule. For example, click the **pen** icon and select **Deny**.
   4. In the **Source** field, select the source addresses of the traffic. For example, **LAN Users**.
   5. In the **Destination** field, select the destination addresses of the traffic. For example, **Internet**.

      The selection of source and destination addresses depends on the forwarding firewall rule set. The address range selected in an application rule must be part of the range specified in the rule set and cannot contain a higher amount of addresses than specified in the forwarding firewall rule.
8. Click **Send Changes** and **Activate**.

Figures

1. app_fb.jpg
2. app_rl.jpg