Application Based Provider Selection

https://campus.barracuda.com/doc/79462966/

You can specify which link is used for an application by creating an application based link selection connection object. In this object configure a default connection policy, add applications or application categories, and then assign them to a connection object for the Internet connection the should use. Applications that are not explicitly defined use the default connection policy.

When a user connects to a service the firewall detects the application and stores the application and the associated destination IP addresses. The first connection for an application always uses the default connection object. Every subsequent connection by this application to the same destination is now sent through the link configured for this application. For some applications that use a wide range of varying destination IP addresses the effectiveness of the application based provider selection may be limited.

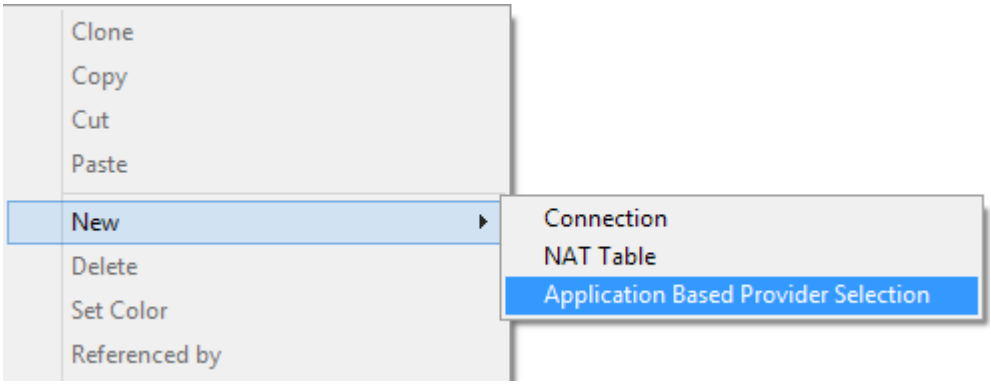
Before You Begin

Before you create an application based link selection connection object, complete the following:

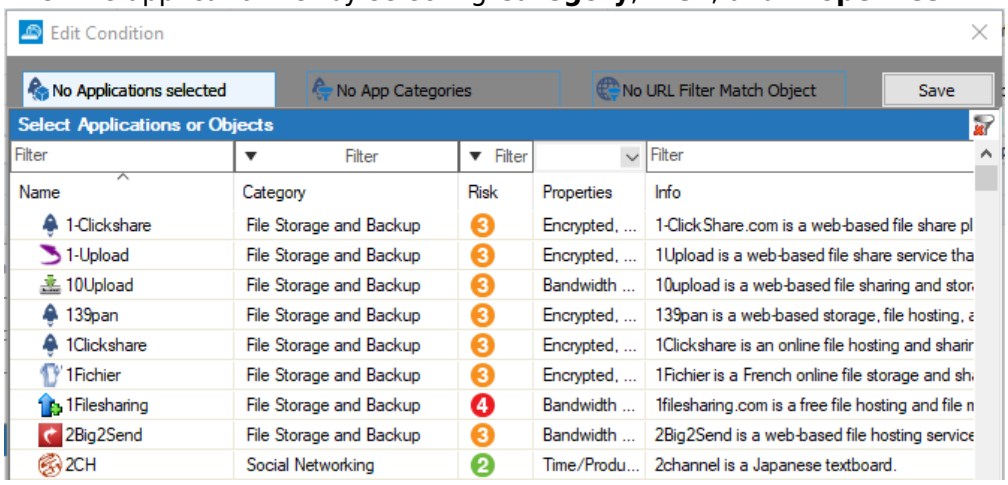
- Enable Application Control. For more information, see Application Control.
- Create connection objects for every WAN connection, you want to route application traffic over. For more information on how to create connection objects, see Connection Objects.

Step 1. Create a Application Link Connection Object

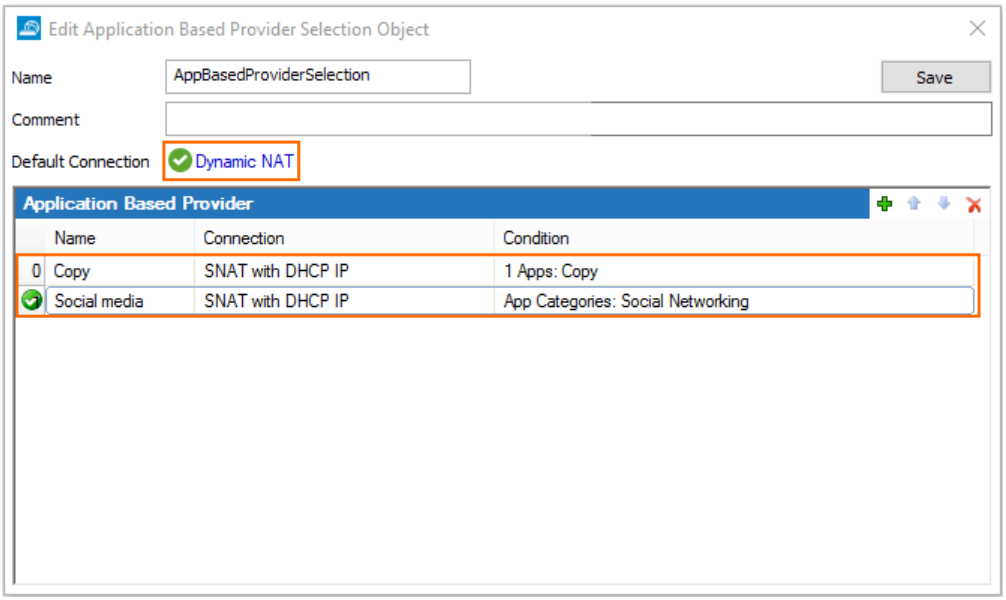
1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. In the left menu, click **Connections**.
3. Click **Lock**.
4. Right-click the table and select **New > Application Based Provider Selection**.



5. In the **Edit Application Based Provider Selection Object** window, specify the following settings:
   - **Name** – Enter a name for the connection object (e.g., `AppBasedProviderSelection`).
   - **Default Connection** – Select the default connection from the list by clicking the link. Traffic that is not defined in the application based links is routed over this connection.
6. For every application or application category that you want to add:
   1. Click the plus sign (**+**) to add an application based link entry.
   2. Edit the **Name** of the new entry.
   3. Select the **Connection Object** for the ISP to route the detected application traffic (e.g., `Source NAT with DHCP` for the first DHCP line).
   4. Double-click the **Condition** field.
   5. In the **Edit Condition** window, click the **No Application selected** tab.
   6. Either add applications from the list by category or double-click the entry. You can also filter the application list by selecting **Category**, **Risk**, and **Properties**.



7. Click **Save**.



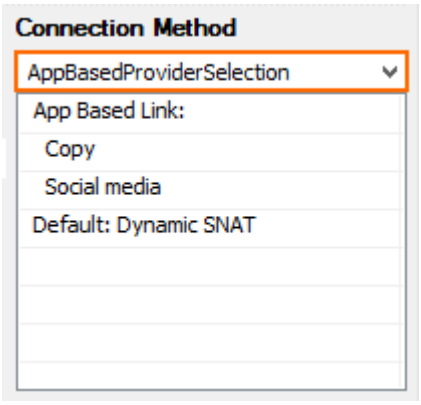
8. Click **Save**.
7. Click **Send Changes** and **Activate**.

The application link connection object is now in the **Connections** list.

Step 2. Create an Access Rule

Create an access rule to redirect the application traffic. Alternatively, you can also edit an existing matching access rule.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Right-click the **Main Rules** table and select **New > Rule**.
4. Create a Pass access rule with the following settings:
   - **Source** – Select **Trusted LAN**.
   - **Service** – Select the type of service.
   - **Destination** – Select **Internet**.
   - **Application Policy** – Select **Application Control** and **SSL Inspection**. If configured, select a policy from the **SSL Inspection Policy** drop-down list. For more information, see SSL Inspection in the Firewall.
   - **Connection Method** – Select the application link connection object that you created in Step 1 (e.g., `AppBasedProviderSelection`).



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

All applications are now routed over the provider selected in the application based link selection object. Go to the **Firewall > History** page to monitor which link is selected for the applications defined in the connection object.

ID	State	IP Protocol	Port	Source	Interface	Destination	Output-IF	Application	Application Context	Rule
		TCP	443	10.0.10.11	eth0	64.235.151.8	dhcp	Copy	push0.copy.com	LAN-2-INTERNET/<App>:A...
		TCP	443	10.0.10.11	eth0	31.13.64.17	dhcp	Facebook Base	www.facebook.com	LAN-2-INTERNET/<App>:A...
		TCP	80	10.0.10.11	eth0	188.40.238.250	eth1	Web browsing	www.eicar.org	LAN-2-INTERNET/<App>:A...

Figures

1. app_based_routing-01.png
2. AppBasedProviderSelection01.png
3. AppBasedProviderSelection02.png
4. AppBasedProviderSelection03.png
5. AppBasedProviderSelection04.png
6. AppBasedProviderSelection05.png