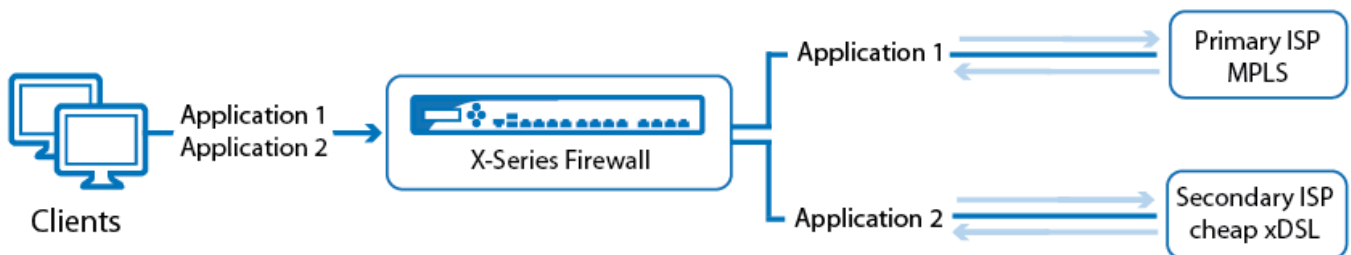


Application Based Connection Objects

<https://campus.barracuda.com/doc/44433945/>

Use application-based connection objects to select the WAN connection based on the application. Add application-based link policies for each application or application category. Each policy can use a different connection object. Traffic that does not match one of these policies is sent using the default connection object.

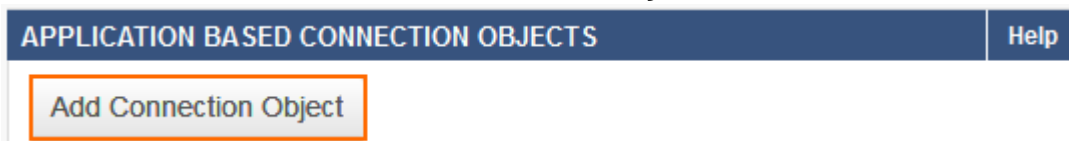


Before you Begin

- (optional) Create custom connection objects for each Internet connection.

Step 1. Create the Application Based Connection Object

1. Go to **FIREWALL > Connection Object**
2. In the **APPLICATION BASED CONNECTION OBJECTS** section, click **Add Connection Object**.



3. Enter a **Name**.
4. Select the **Default Connection**.

Add Application Based Connection Object ?


Name:	<input type="text" value="AppBasedConnObject"/>
Description:	<input type="text" value="Enter a description for this Object"/>
Default Connection:	<input type="text" value="Default (SNAT)"/>

Connection used if none of the criteria defined below match. Default: Dynamic SNAT

5. Click **Save**.

Step 2. Add Application Based Link Policies

Edit the application-based connection object you just created and add the application-based link policies. Applications can be added individually, through the application browser, or by application category. All selected applications will use the connection object selected for this policy.


1. Stay on the **FIREWALL > Connection Object** page.
2. Click  to edit the application-based connection object you created in Step 1.
3. Click **Add**. The **Add Application Based Link Policy** pop-over opens.

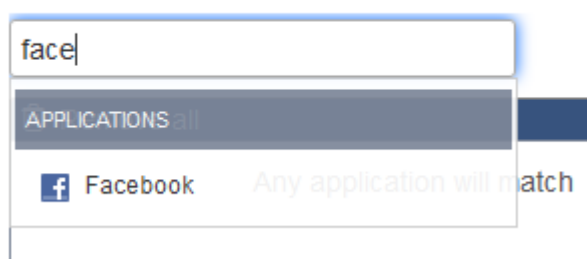
Application Based Links:

Add


Name	Connection	Applications	Categories	Actions
No data available in table				














4. Select the connection object from the **Connection** dropdown.
5. Add applications to the links policy by name, application browser and/or category:
 - Start typing the application name in the **Select applications** textbox and then click on the application from the list.

Applications 



- Click **Browse** to select the applications in the application browser.
- Select the application categories from the **Categories** list.

Categories  clear

	Uncategorized	<input type="checkbox"/>
	Standard Network	<input type="checkbox"/>
	File Sharing P2P	<input checked="" type="checkbox"/>
	VOIP	<input type="checkbox"/>
	Conferencing	<input type="checkbox"/>
	Instant Messaging	<input type="checkbox"/>
	Media Streaming	<input type="checkbox"/>
	Proxies and Anonymizers	<input type="checkbox"/>
	Tunneling	<input type="checkbox"/>
	File Storage and Backup	<input type="checkbox"/>
	Games	<input type="checkbox"/>
	Mobile	<input type="checkbox"/>
	Business	<input type="checkbox"/>

6. Click **Save**.

The application-based link policy is now listed in the in the application-based connection object.

Name	Connection	Applications	Categories	Actions
Facebook	Dynamic SNAT	 Facebook		  
FileSharing	SNAT with DHCP IP		 File Sharing P2P	  


Step 3. Edit the Access Rule to use the Application Based Connection Object

1. Go to **FIREWALL > Firewall Rules**.
2. Double-click on the access rule you want to use the Application Based Connection Object. The **Edit Access Rule** pop-over opens. E.g., **LAN-2-INTERNET**
3. Select the application-based connection object created in Step 1 from the **Connection** dropdown.

Edit Access Rule ?

General **Advanced**

Action:
Allow



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:
LAN-2-INTERNET

Description:
Allows internet access from Trusted LAN for typical applications.

Connection:
AppBasedConnectionObject

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
Ref: Trusted LAN

Network Services
Any
Any

Destination
Any
Ref: Internet

4. Click **Save**.

To check which outgoing interface is used for a connection, go to **BASIC > Active Connections** or **BASIC > Recent Connections** and check the **SNAT** column.

Figures

1. app_based_provider.png
2. abc01.png
3. abc02.png
4. edit.png
5. abc03.png
6. abc04.png
7. abc05.png
8. abc06.png
9. abc07.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.