

## How to Configure Link Protection for Mail Security in the Firewall

<https://campus.barracuda.com/doc/96026311/>

Link Protection protects users from fraudulent links inside of plain-text and HTML emails. This cloud-based service requires an active Advanced Threat Protection (ATP) subscription.

### Step 1. Activate Link Protection Globally on the Firewall

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Security Policy**.
2. Click **Lock**.
3. In the **Mail Security** section, enable Link Protection:
  - **Enable Link Protection** – Select from the list:
    - **Yes** – Enables link protection as soon as you click **Send Changes / Activate**.
    - **No** – Disables link protection as soon as you click **Send Changes / Activate**.
    - **Auto** – If CGF policies are licensed, link protection is automatically enabled once CGF policies are enabled.
  - **Link Protection Domain Allow List** – Enter the domain names you want to exclude from being evaluated by Link Protection. The wildcards \* and ? are allowed.


**Mail Security**

	Mail Server SSL Certificates		
	<table><thead><tr><th>IP Address</th><th>SSL Certificate</th></tr></thead><tbody></tbody></table>	IP Address	SSL Certificate
IP Address	SSL Certificate		
DNSBL Server	<input type="text" value="b.barracudacentral.org"/>		
Prefix for the subject	<input type="text"/>		
Enable Link Protection	<input type="text" value="Yes"/>		
Link Protection Domain Allow List	<div><div>???google.com</div></div>		

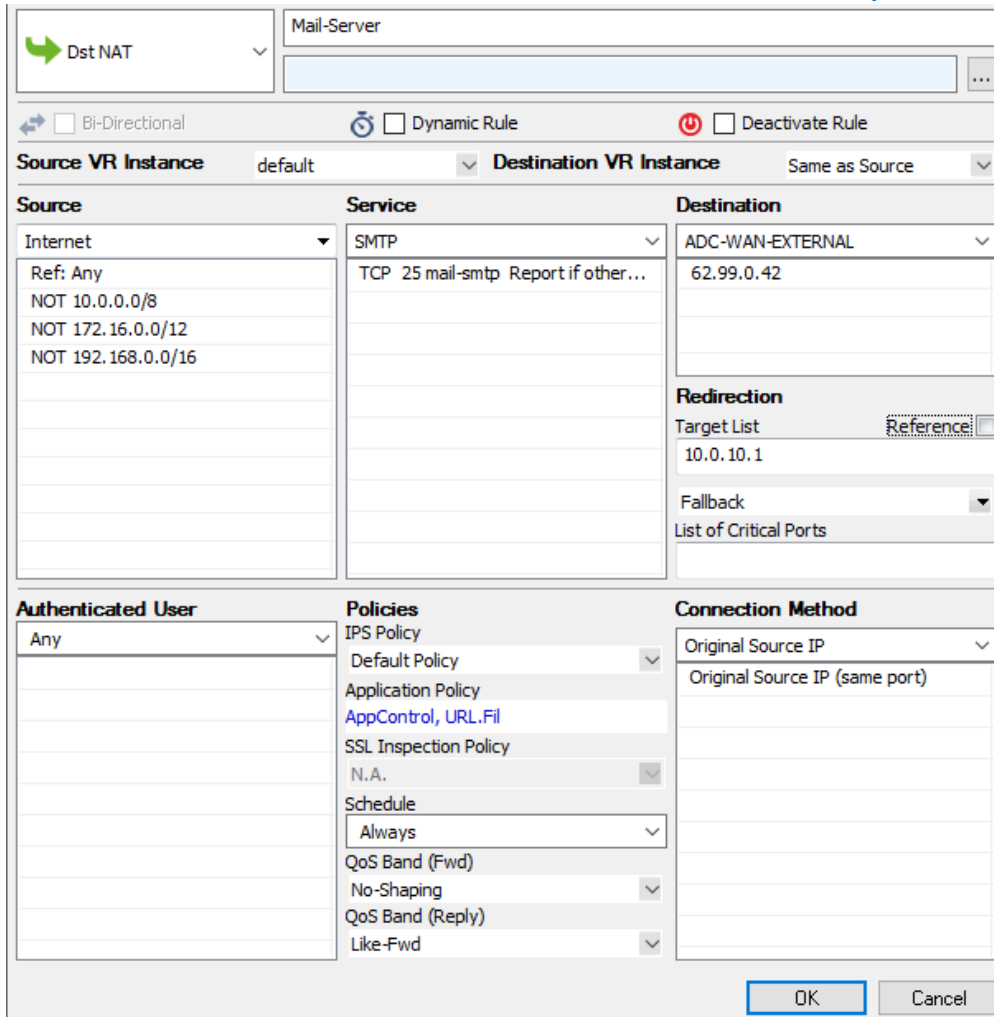
4. Click **Send Changes** and **Activate**.

**Step 2. Create a Dst NAT Access Rule to Forward Mail Traffic to the Mail Server**

A **Dst NAT** access rule redirects SMTP traffic sent to an external IP address to a destination on the internal network.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Either click the plus icon (+) at the top right of the ruleset, or right-click the ruleset and select **New > Rule**.  

4. Select **Dst NAT** as the action.
5. Enter a **Name** for the rule. For example, Mail - Server.
6. Specify the following settings that must be matched by the traffic to be handled by the access rule:

- **Source** – The source addresses of the traffic.
- **Destination** – The destination addresses of the traffic.
- **Service** – Select **SMTP**.
- **Target List** – Enter the internal IP of your mail server.
- **Connection Method** – For more information, see [Connection Objects](#).



The screenshot shows the configuration window for a rule named "Mail-Server". At the top, there is a "Dst NAT" dropdown with a green arrow icon. Below this are checkboxes for "Bi-Directional", "Dynamic Rule", and "Deactivate Rule". The "Source VR Instance" is set to "default" and the "Destination VR Instance" is set to "Same as Source".

The main configuration area is divided into three columns: "Source", "Service", and "Destination".

- Source:** A dropdown menu shows "Internet". Below it, a list of source addresses is displayed: "Ref: Any", "NOT 10.0.0.0/8", "NOT 172.16.0.0/12", and "NOT 192.168.0.0/16".
- Service:** A dropdown menu shows "SMTP". Below it, the text "TCP 25 mail-smtp Report if other..." is visible.
- Destination:** A dropdown menu shows "ADC-WAN-EXTERNAL". Below it, the IP address "62.99.0.42" is listed.

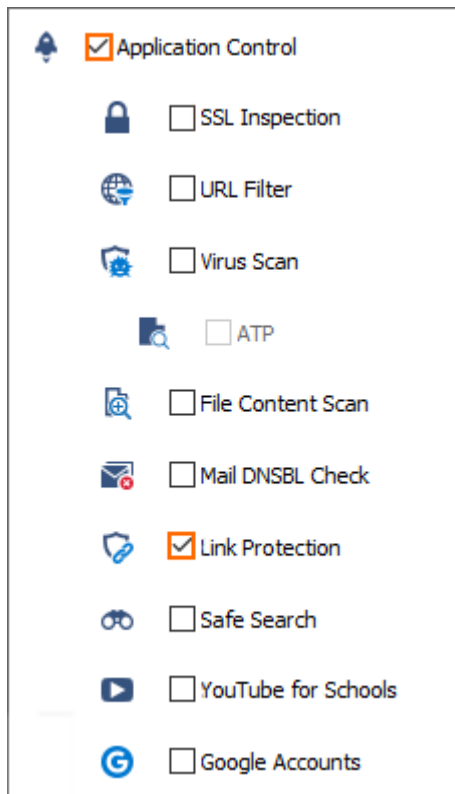
Below the main configuration area, there are three more sections:

- Authenticated User:** A dropdown menu shows "Any".
- Policies:** A list of policies is shown, including "IPS Policy", "Default Policy", "Application Policy", "AppControl, URL.Fil", "SSL Inspection Policy", "N.A.", "Schedule", "Always", "QoS Band (Fwd)", "No-Shaping", "QoS Band (Reply)", and "Like-Fwd".
- Connection Method:** A dropdown menu shows "Original Source IP". Below it, the text "Original Source IP (same port)" is visible.

At the bottom right, there are "OK" and "Cancel" buttons.

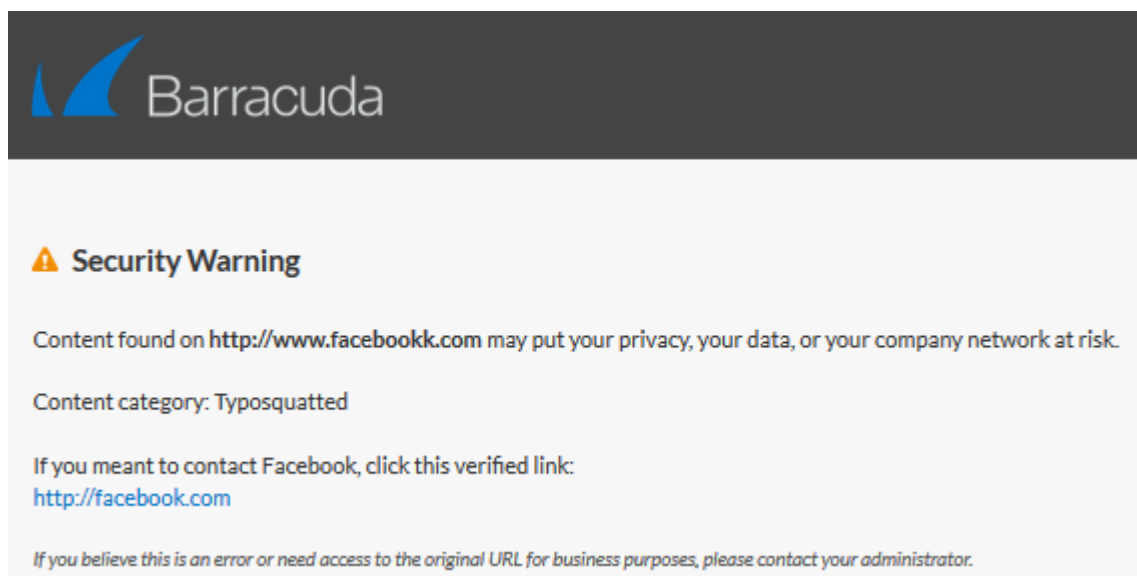
#### 7. In **Application Policy**:

- **Application Control** – Select the check box. For more information on all Application Control features, see [Application Control](#).
- **Link Protection** – Select the check box.



8. Click **OK**.
9. Drag and drop the access rule so that it is the first rule that matches the traffic that you want it to forward. Ensure that the rule is located *above* the BLOCKALL rule; rules located below the BLOCKALL rule are never executed.
10. Click **Send Changes** and **Activate**.

Your firewall is now configured to handle embedded WEB-links inside of plain-text and HTML emails. In case Link Protection detects a fraudulent URL, you will be redirected to a Security Warning page that will show up in your web browser, i.e.:



## Figures

1. activate\_globally\_lp\_01.png
2. FW\_Rule\_Add\_01.png
3. add\_access\_rule\_redirect\_01.png
4. enable\_application\_rule\_for\_lp\_01.png
5. securit\_warning\_page\_01.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.