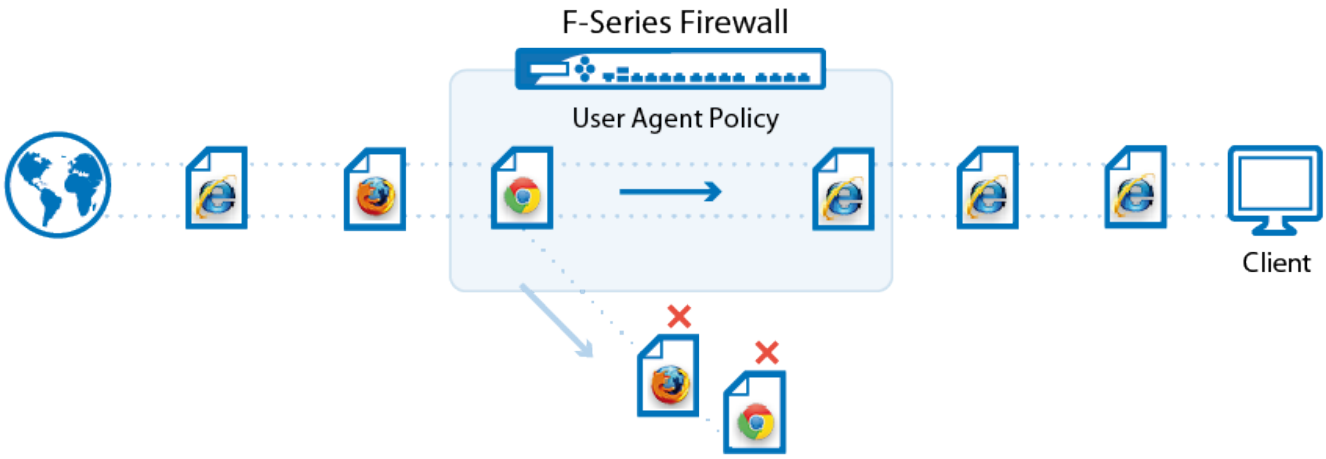
How to Configure User Agent Filtering in the Firewall

The NextGen Firewall F-Series can filter HTTP and HTTPS traffic based on the user agent string of the browser. For this policy to apply, web traffic must match an access rule with Application Control and an application rule with a User Agent policy.



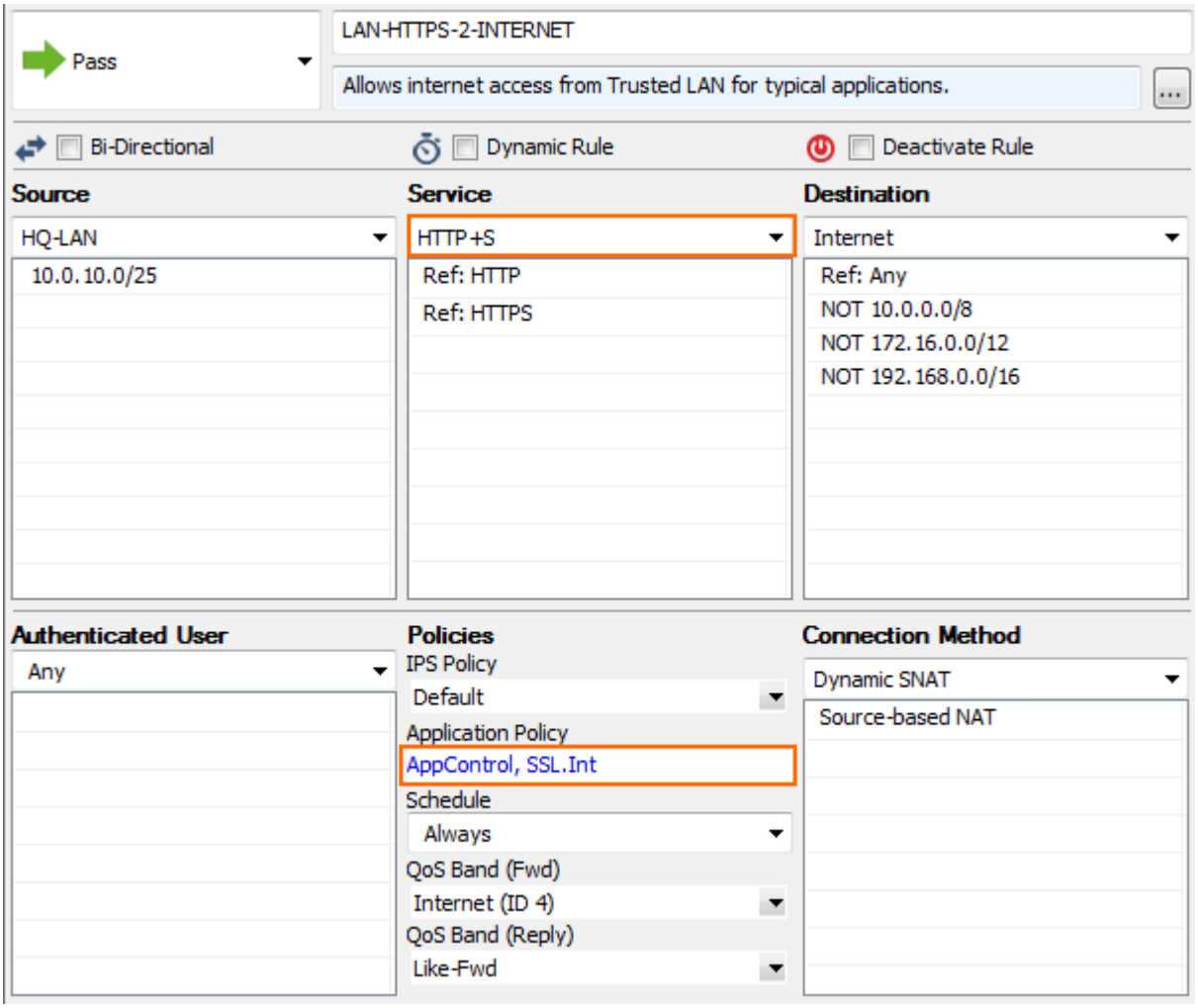
Before You Begin

- Enable Application Control. For more information, see How to Enable Application Control
- Create User Agent Policies. For more information, see How to Create User Agent Policies.

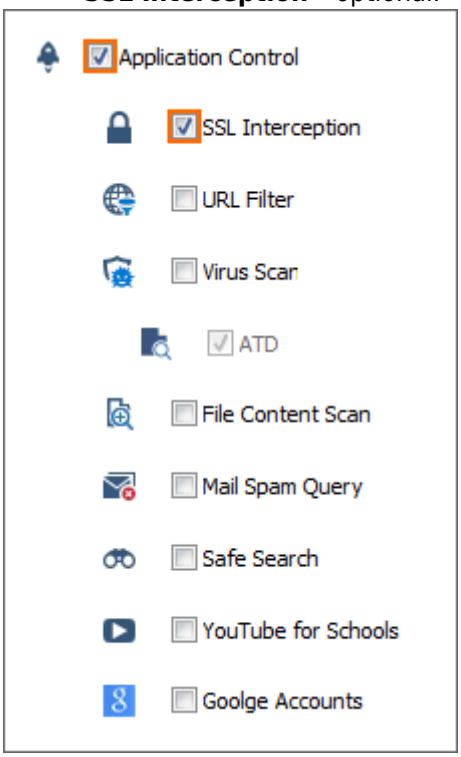
Step 1. Create an Access Rule to Match Web Traffic

Create a PASS access rule to match HTTP and HTTPS traffic and enable Application Control and, optionally, SSL Interception.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Firewall > Forwarding Rules**.
2. Double-click to edit the access rule matching HTTP/HTTPS traffic.



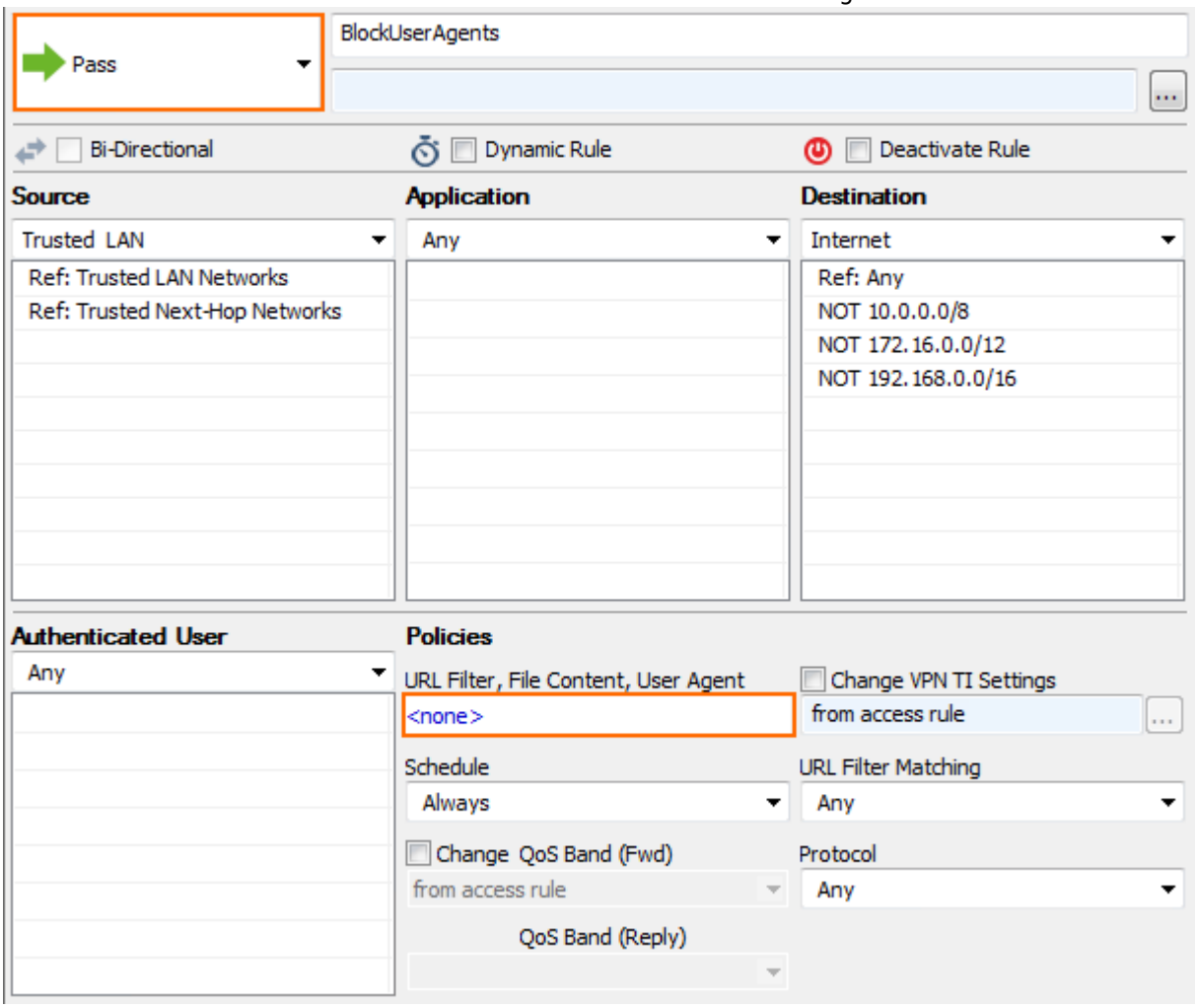
3. Click on the **Application Policy** link and select:
   - **Application Control** – required.
   - **SSL Interception** – optional.



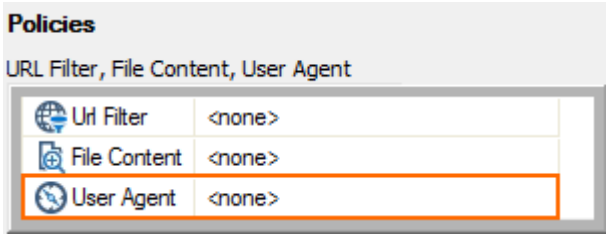
4. Click **OK**.
5. Click **Send Changes** and **Activate**.

Step 2. Create Application Rule using User Agent Policies

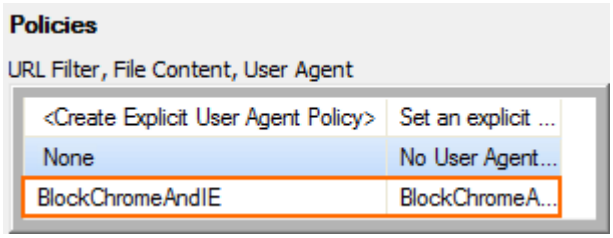
1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Firewall > Forwarding Rules**.
2. In the left menu, click **Application Rules**.
3. Click **Lock**.
4. Create a **PASS** application rule. For more information, see How to Create an Application Rule.
   - **Source** – Select the same source used in the matching access rule.
   - **Application** – Select **Any** to configure only the filter policies. Otherwise, select an application object from the drop-down list to combine Application Control and User Agent filtering.
   - **Destination** – Select the same destination used in the matching access rule.



5. Click the **URL Filter, File Content, User Agent** link.

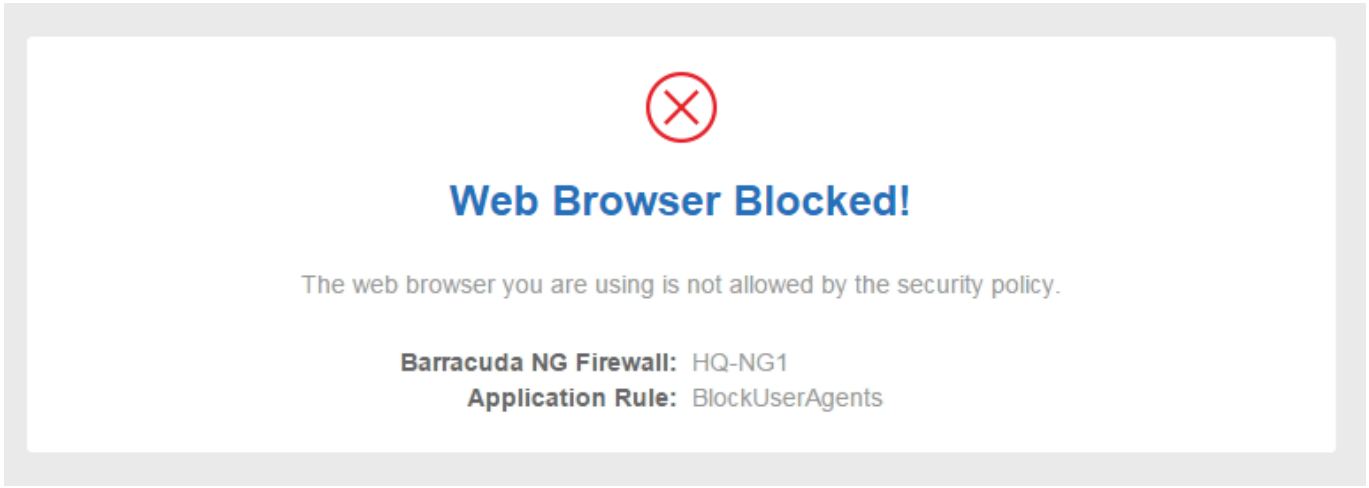


6. Click **User Agent**.
7. Select a user agent policy from the list. For more information, see How to Create User Agent Policies.



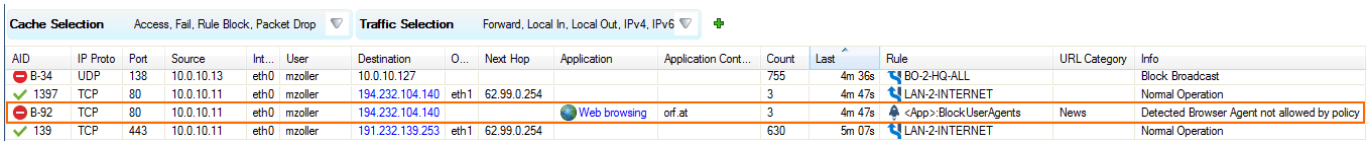
8. Click **OK**.
9. Click **Send Changes** and **Activate**.

When users attempt to access a service with a web browser that is not allowed in the user agent policy, the connection is either reset or redirected to a custom block page. The block page is customizable. For more information, see How to Configure Custom Block Pages and Texts.



Monitoring

To monitor blocked connections, go to **FIREWALL > History** and check the **Info** column of blocked connections for **Detected Browser Agent not allowed by policy**.



Figures