How can we enable Strict Authentication for unauthenticated users?

Applicable to Version: 10.00 onwards

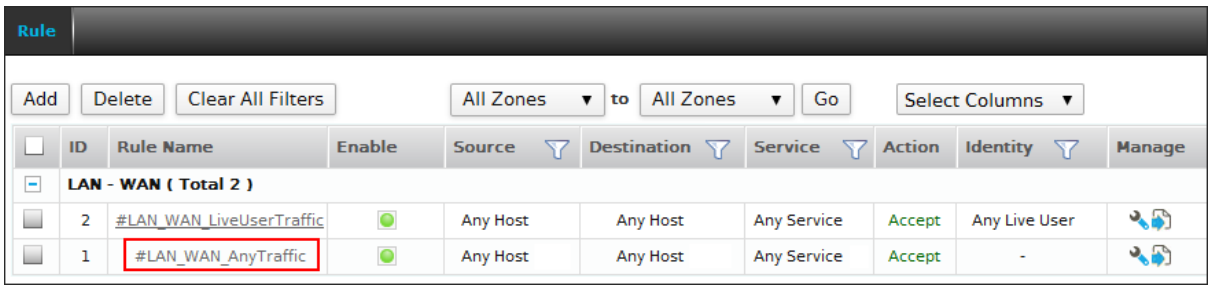
Overview

Firewall rules control what network traffic is allowed and what traffic is disallowed to and from your Appliance. Depending on the rule, Appliance decides how to process the access request. When Appliance receives the request, it checks for the source address, destination address and the services, and tries to match with the firewall rule. If Identity match is also specified, firewall checks whether the user is allowed access or not. It searches in the Live User Connections List, if user is found, and all other matching criteria are fulfilled, access is allowed or denied based on the action configured in the rule.

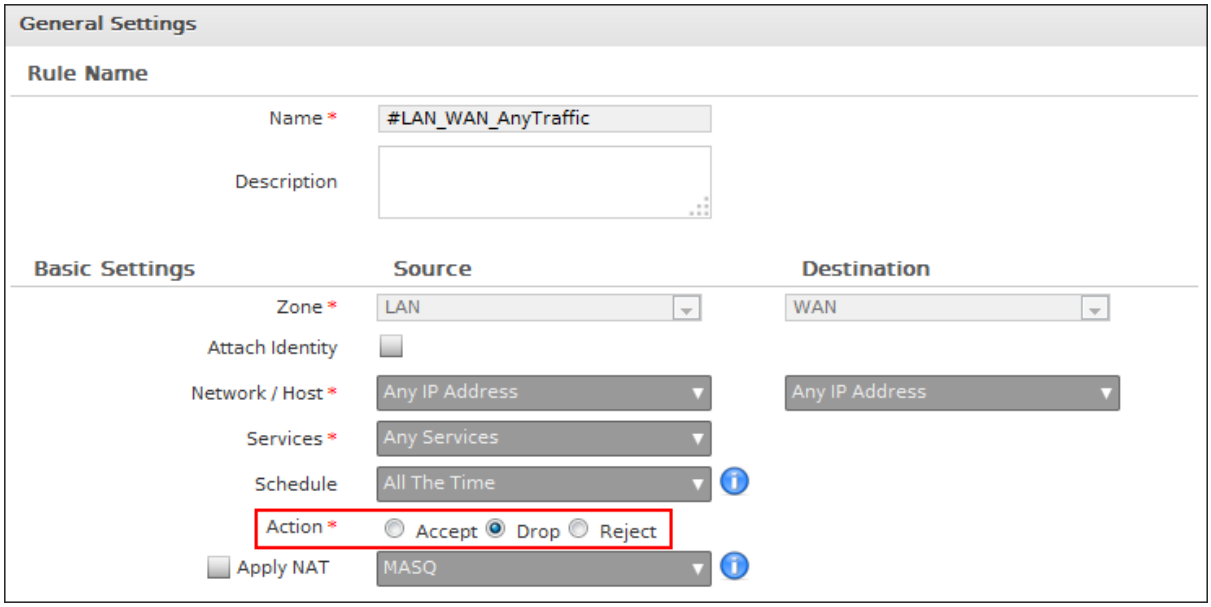
Firewall Rule Configuration

You can enable Strict Authentication by configuring the Default Rule 1: LAN_WAN_AnyTraffic to drop all traffic. By doing this, any unauthenticated user trying to browse the Internet will have to authenticate via the Captive Portal or other relevant Cyberoam Client.

To configure firewall rule, go to **Firewall > Rule > Rule** to add or edit firewall rules. Default Firewall Rules are shown in the below screen:



Set Action as **Drop** in **Default Rule 1: LAN_WAN_AnyTraffic**, as shown below.



Click **OK** to update the firewall rule.

Note:

- Default Firewall rules can be modified as per the requirement but cannot be deleted.
- End Clients/Systems using Public DNS must use Firewall Rules to bypass DNS traffic.

Document Version: 2.0 – 13 November, 2013