Intro to Firewalls Workout Instructions

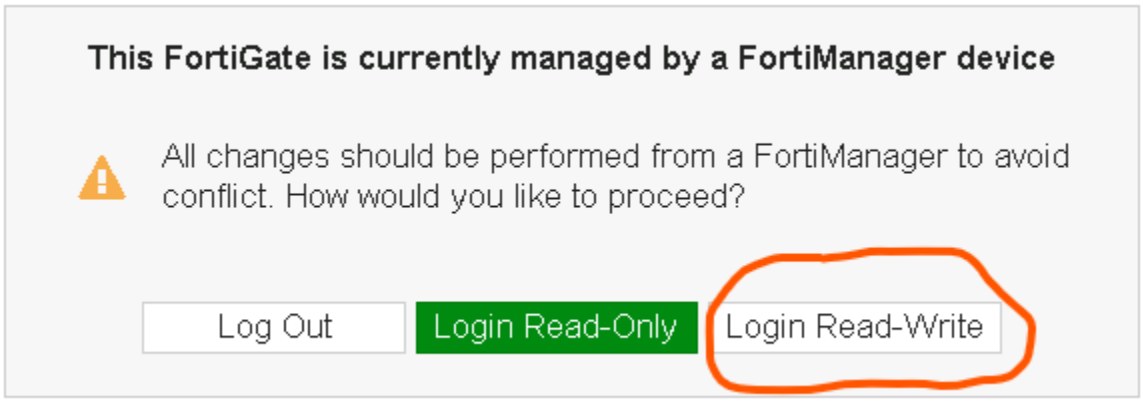
In this workout, you will learn the basics of working with firewalls. Fortinet manufactures high-end, next-generation firewalls, and we offer this workout opportunity through their generosity. You will work with a real industry firewall common to many companies.

Login to your firewall by first logging in through the guacamole server. Then open a browser in your guacamole server and go to https://10.1.1.10 (in your browser, click Advanced and then scroll down to click “Accept risk and Continue”).

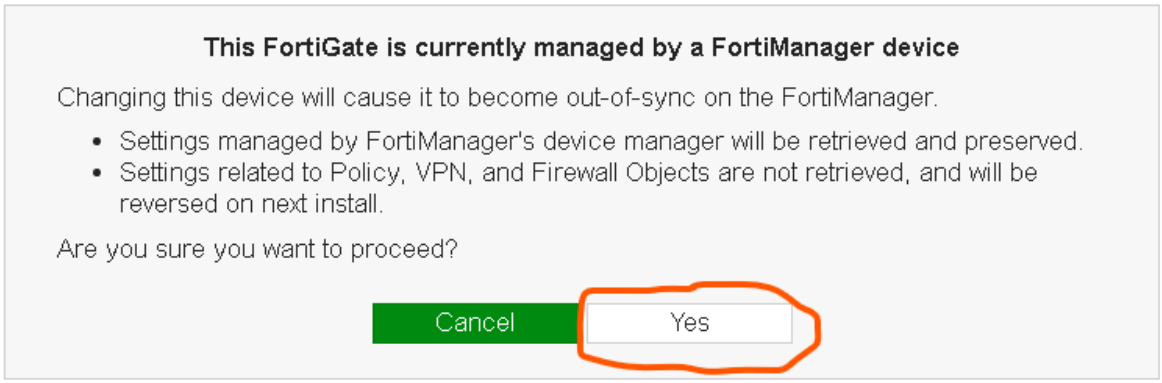
You will log in with the following credentials:

- Username: *admin*
- Password: *Let’s workout!*

It’s possible that you’ll receive a notice that your license is still being validated. This may take a few minutes to complete. Once complete and logged in, you’ll first see the following prompt. Click to *Login Read-Write*

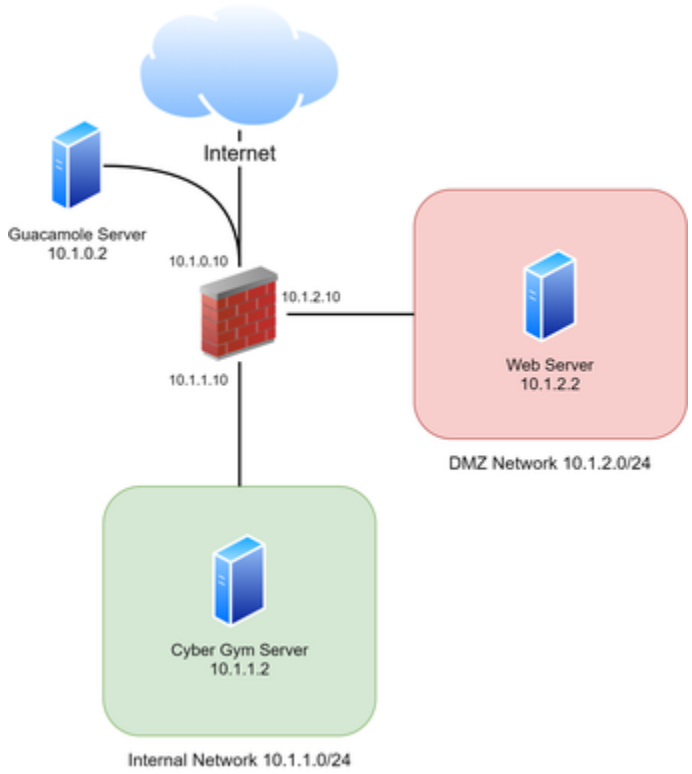


You will then see a warning about the device being managed by a Fortimanager device. In practice, you would use only the FortiManager to make changes to a firewall, but for this workout, you’ll want to edit the firewall directly. Click *Yes* here.



Finally, you'll receive a prompt about registering the device. Click *Later*.

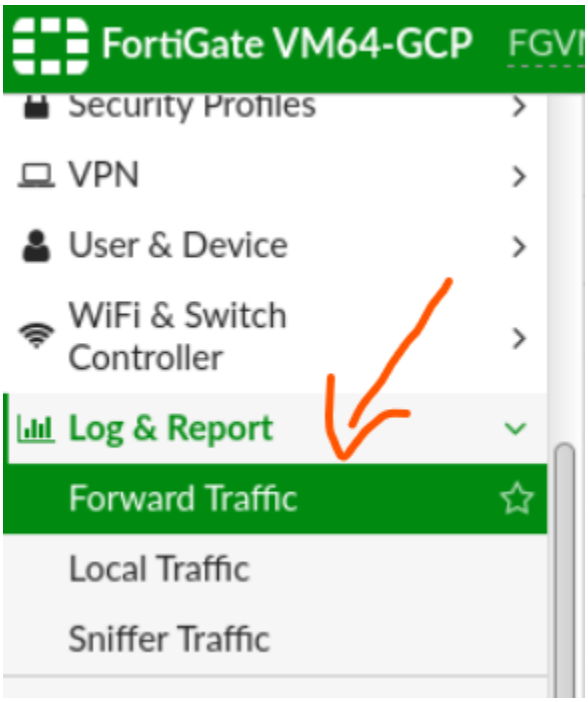
A diagram of your workout is shown below. You will work on the Cyber Gym server (IP address 10.1.1.2) and configure the firewall to restrict traffic between the DMZ network and internal network.



Your Mission

Task 1: For this mission task, you need to completely block traffic coming from the DMZ to the Internal Network. A port scan will occur regularly from the DMZ into the inbound network. First, observe the port scan traffic and identify the host from

which the traffic originates. You can do so by going into the *Forward Traffic Logs* in the location shown below. Observe the source network sending the scan traffic.



Then, block the traffic by editing the correct policy in IPv4 policy. This workout should automatically assess your completion when the port scan traffic can no longer reach the internal network.

Task 2: For this mission task, you want to allow VNC (including port TCP/5901 and ICMP) traffic through the firewall from the server sending the port scan traffic to your internal Cyber Gym server. This task will also auto-complete when you have successfully configured the firewall rule.