Firewall KISS

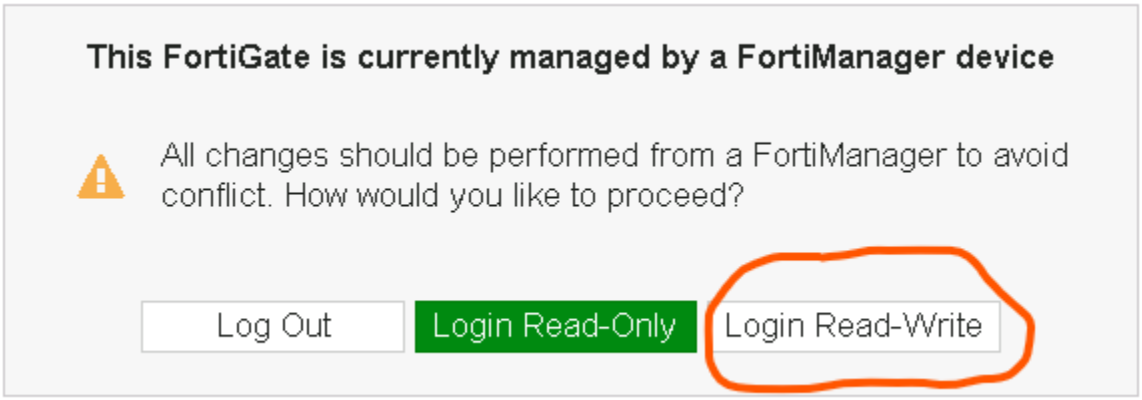
In this workout, you will learn the Keep it Simple principle of security by managing a firewall. You will work with a real industry firewall common to many companies. Fortinet manufactures high-end, next-generation firewalls, and we offer this workout opportunity through their generosity.

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”).

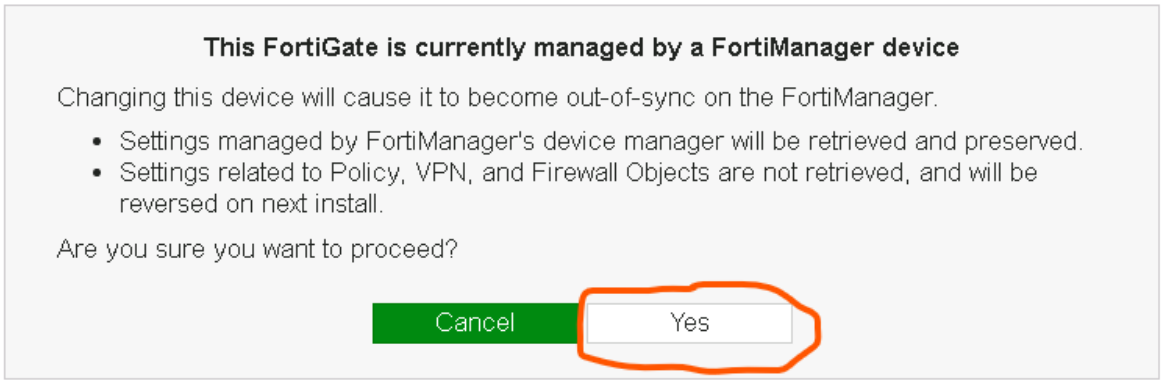
You will log in with the following credentials:

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

When you’ve logged in, you’ll first see the following prompt. Click to *Login Read-Write*

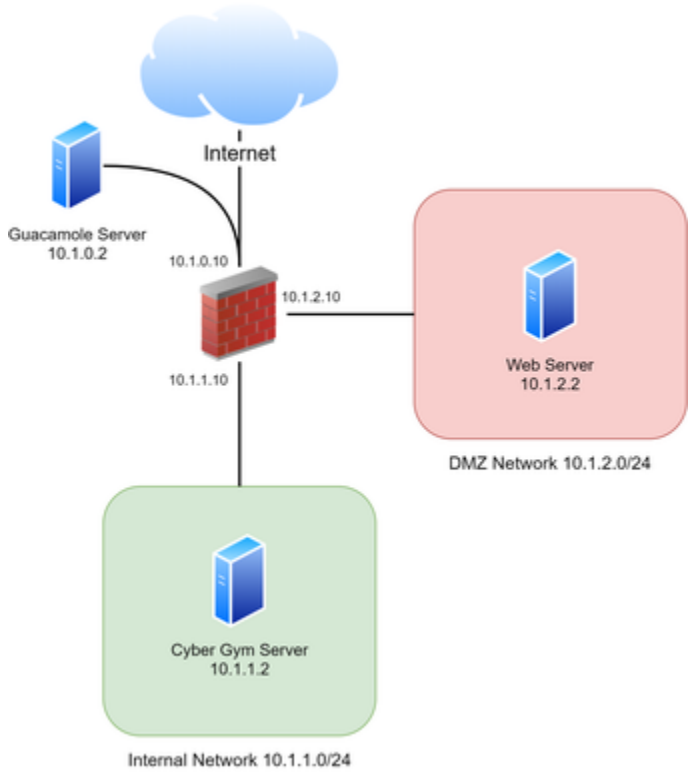


You will then see a warning about the device being managed by a Fortimanager device. In practice, you would use only the FortiManager to make changes to a firewall, but you’ll want to edit the firewall directly for this workout. Click *Yes* here.



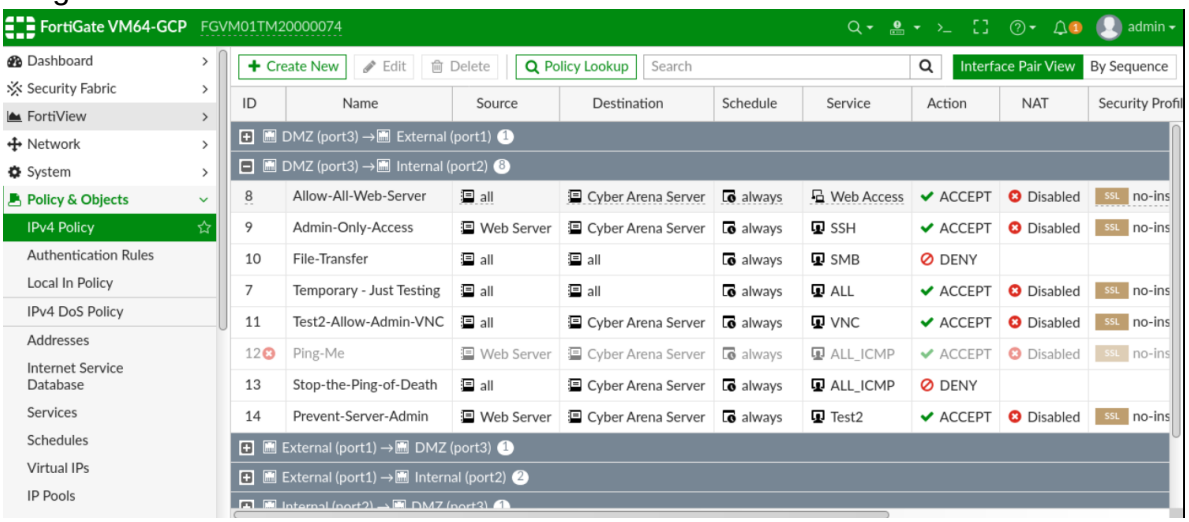
Finally, you'll receive a prompt about registering the device. Click *Later*.

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 Demilitarized Zone (DMZ) network and the internal network.

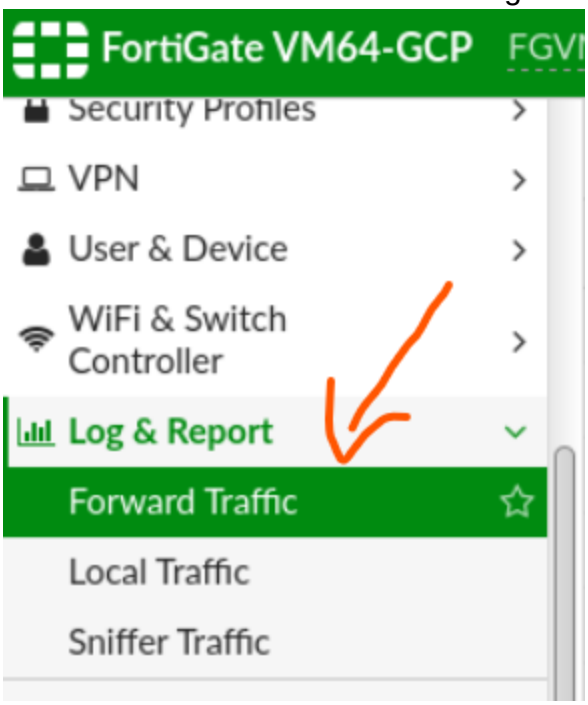


Your Mission

Task 1: For this mission task, you need to completely block traffic coming from the DMZ to the Internal Network. Go to *Policy & Objects* *IPv4 Policy*, and you will see a mess of firewall rules from the DMZ to the Internal Network, as shown in the image below.



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.

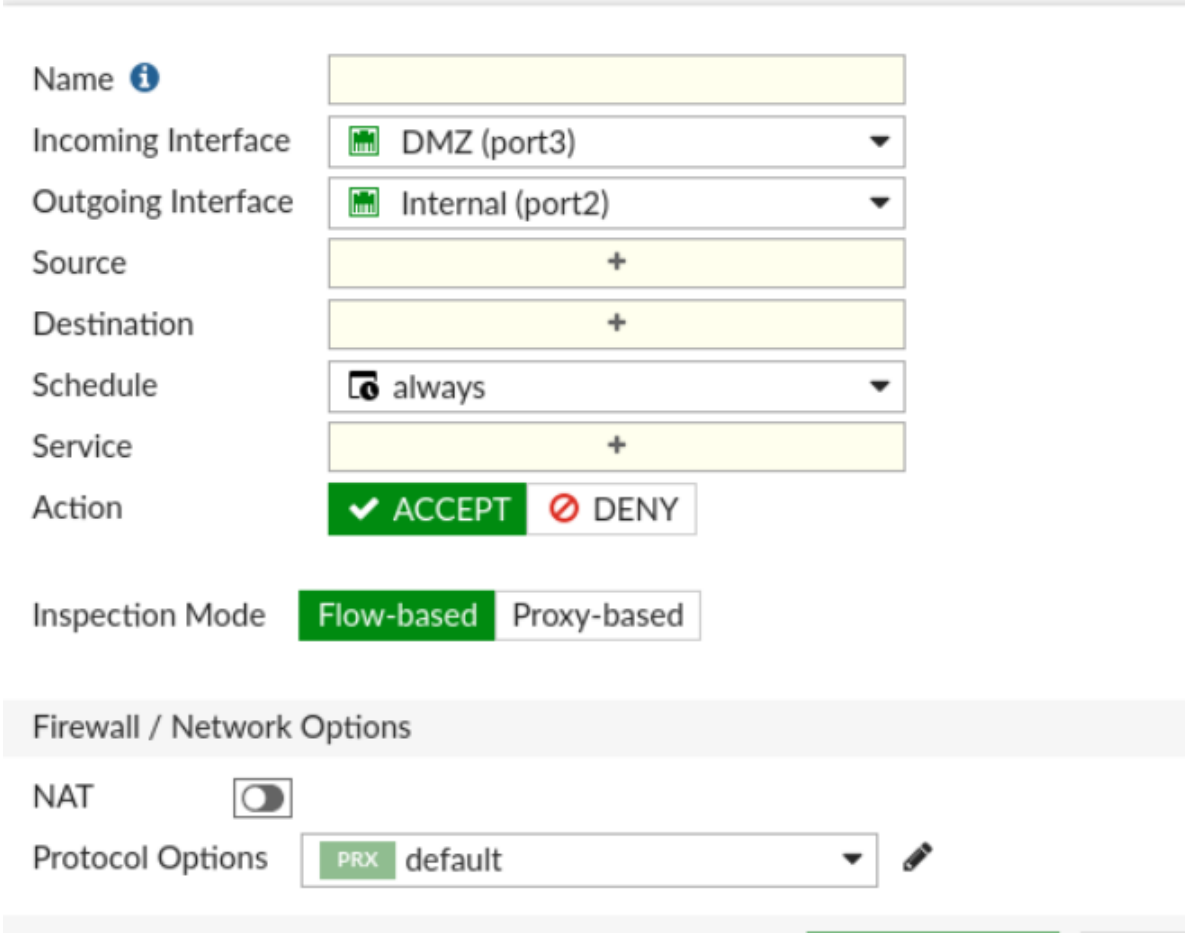


Then, block the traffic by editing the rules in the IPv4 policy. You can delete rules if you are confident they no longer serve a purpose. You can also disable rules by right-clicking the rule and clicking *Set Status Disable*.

This workout will automatically assess your completion when the port scan traffic can no longer reach the internal network. You can see this marked complete from your landing page.

Task 2: For this next mission task, you want to allow VNC (including port TCP /5901) and Ping traffic through the firewall from the server sending the port scan traffic to your internal Cyber Gym server.

To add a firewall rule, click the *Create New* button. You'll want to begin by naming the rule, and setting the Incoming and Outgoing interfaces to DMZ and Internal, respectively, as shown below.



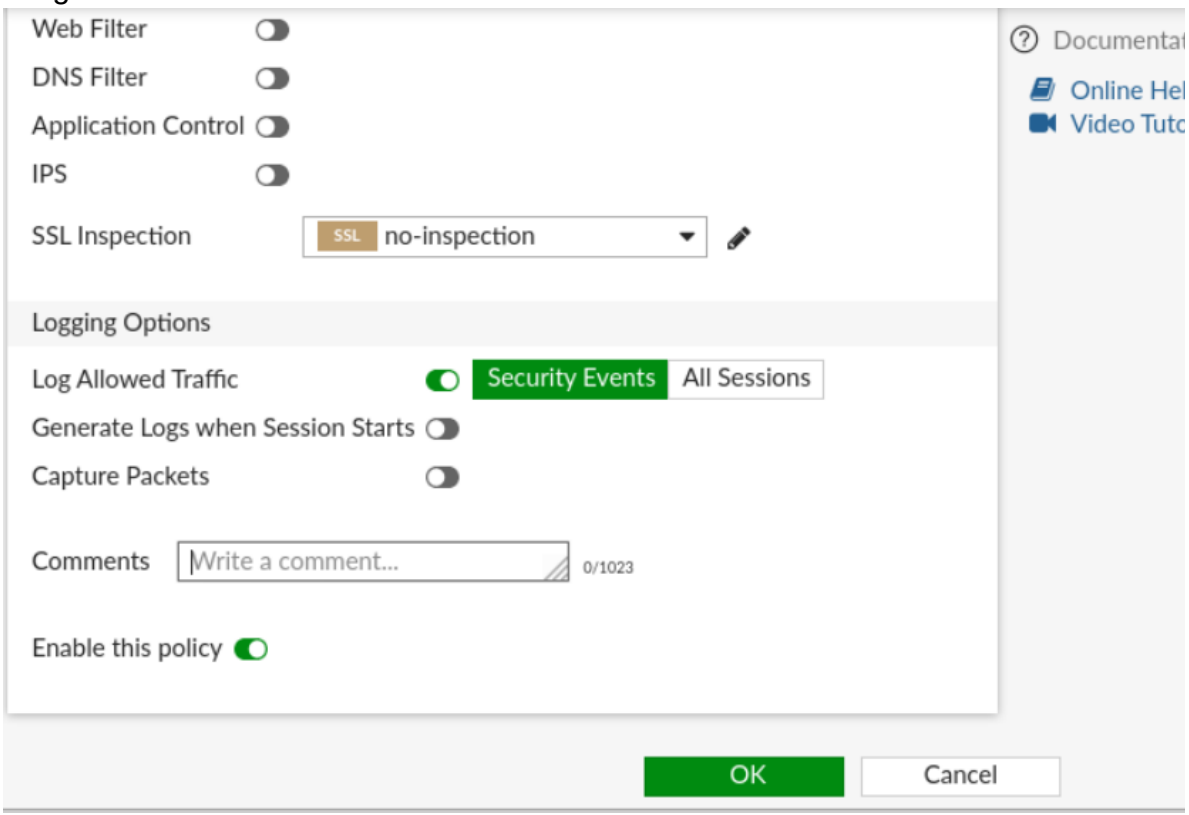
Make sure to disable the Network Address Translation (NAT). Our firewall rules will not need the NAT for this workout.

This task will also auto-complete when you have successfully configured the firewall rule.

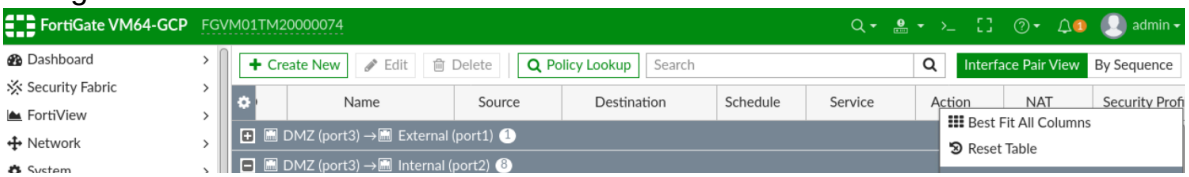
Task 3: Finally, you want to apply the *Keep it Simple* principle to managing this firewall and clean up the rules from the DMZ to the Internal network. Use the following principles to create the firewall rule:

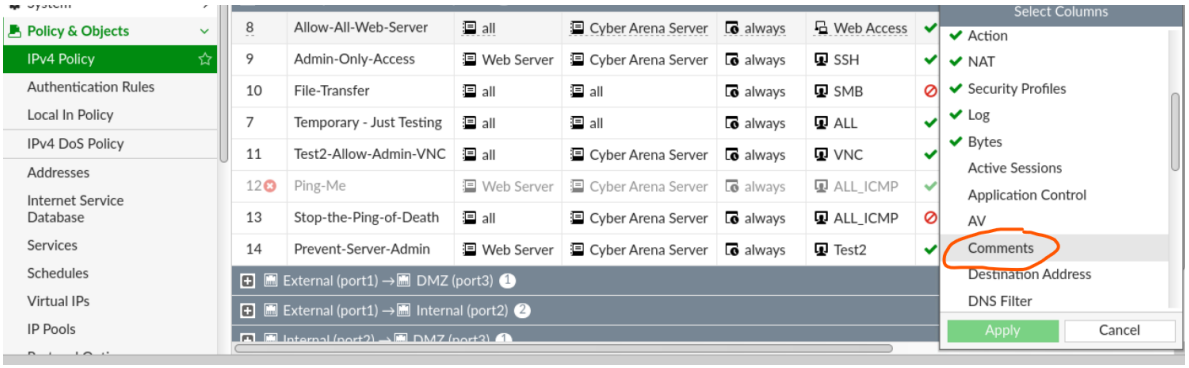
- **Descriptive Naming** - Name the rule based on the traffic it allows. Make it easy for anyone reviewing the rule to understand what it does
- **Grouped Rules** - You should have a single rule when everything is finished that provides the necessary access
- **Commented Rules** - Include the date, your initials, and a short description of the rule for people to easily understand later

To comment on a rule, scroll further to the bottom and use the field shown in the image below.



Before you take a screenshot, add the comments to the column view as shown in the figure below.





Finally, take a screenshot of the rule and upload it for the assessment.