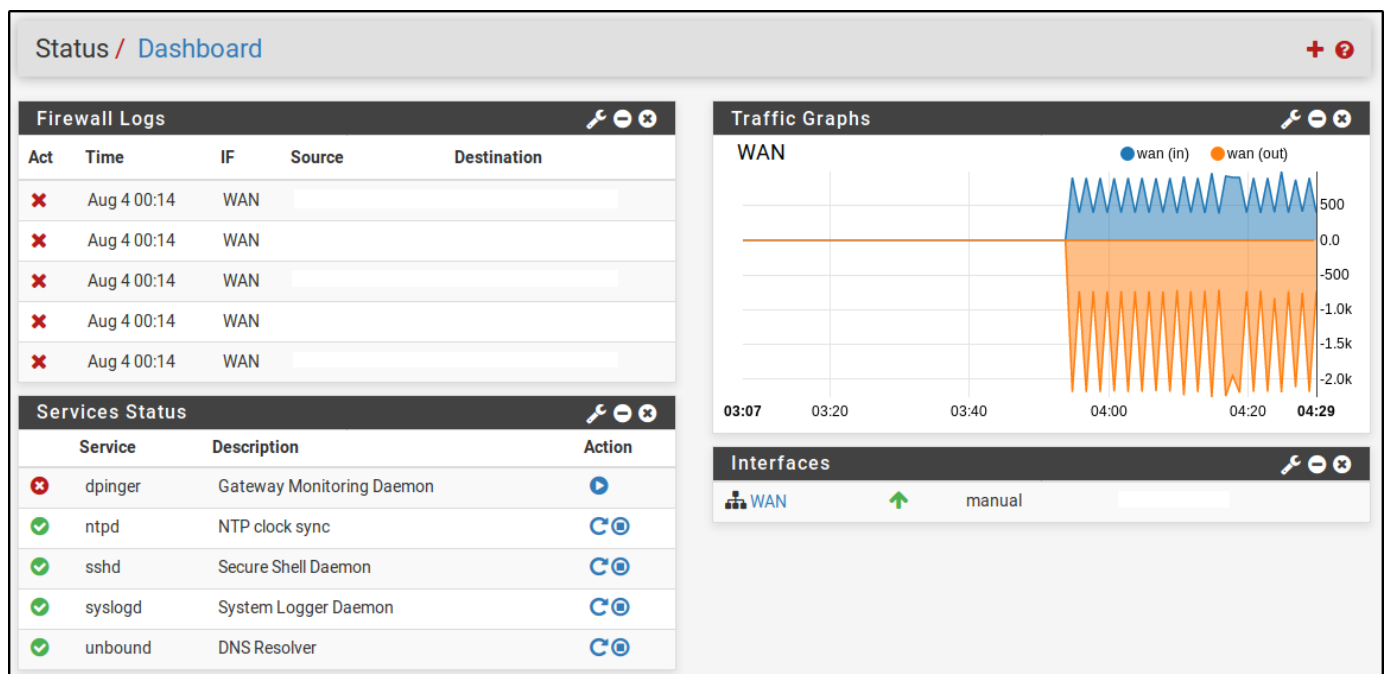


Your team has informed you that the pfSense box be may be running in a default configuration which makes gaining access easy. Use this information to your advantage and gain access to the pfSense configuration panel before moving on.



### pfSense Configuration Panel Overview

After logging into the pfSense configuration panel, we are greeted by a dashboard showing the status of the firewall. This configuration panel gives us a lot of information and a lot of power. We can view and alter the way that the firewall acts as well as monitor the status of the network. To use pfSense to our advantage we will look for a command prompt or web shell to execute commands and get a reverse shell on the machine.



*pfSense configuration panel*

## Web Shells Overview

Traditionally, web shells have represented to some extent a means to an end, however, they can also be used in more permanent scenarios. Common implementations include simple command execution, simple reverse shells that can be 'caught' with netcat, and more complex meterpreter shells. Provided that you are not starting with something like a meterpreter shell, you'll likely move into upgrading shortly thereafter. One important note, websites typically run as a low privileged user such as www-data, so be prepared to move into privilege escalation following gaining your shell.

## Finding an Attack Vector

In order to execute commands in a web app, we first need to find our vector that executes these commands. The web shell can be a command line interface directly integrated into the web server, a limited functionality shell, or a PHP command execution shell. In the case of pfSense, it can execute commands in a command prompt as well as PHP Commands.



*pfSense PHP command execution web shell*

Answer the questions below

What username was used to access the configuration portal?

Correct Answer

What password was used to access the configuration portal?

Correct Answer

What menu tab contains a command prompt tab in the PFSense Configuration panel?

Correct Answer