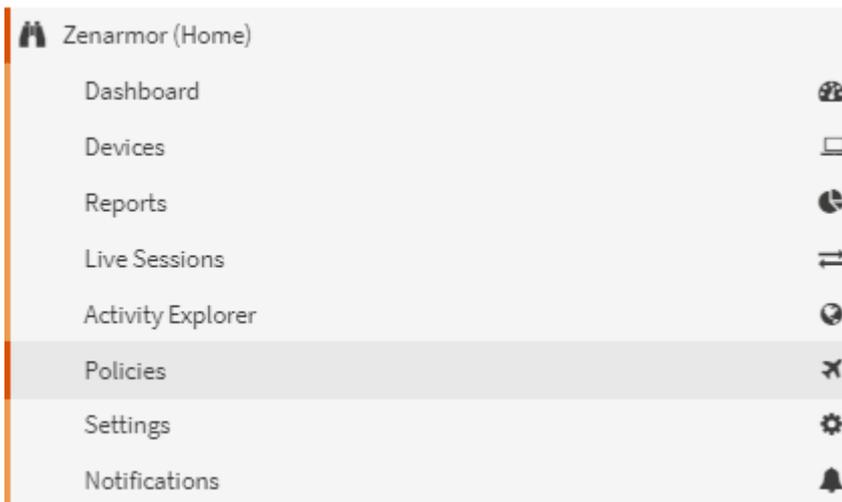
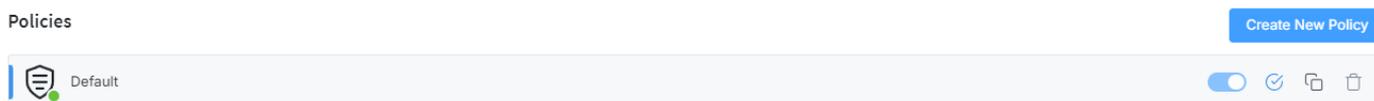


Policies & Rules

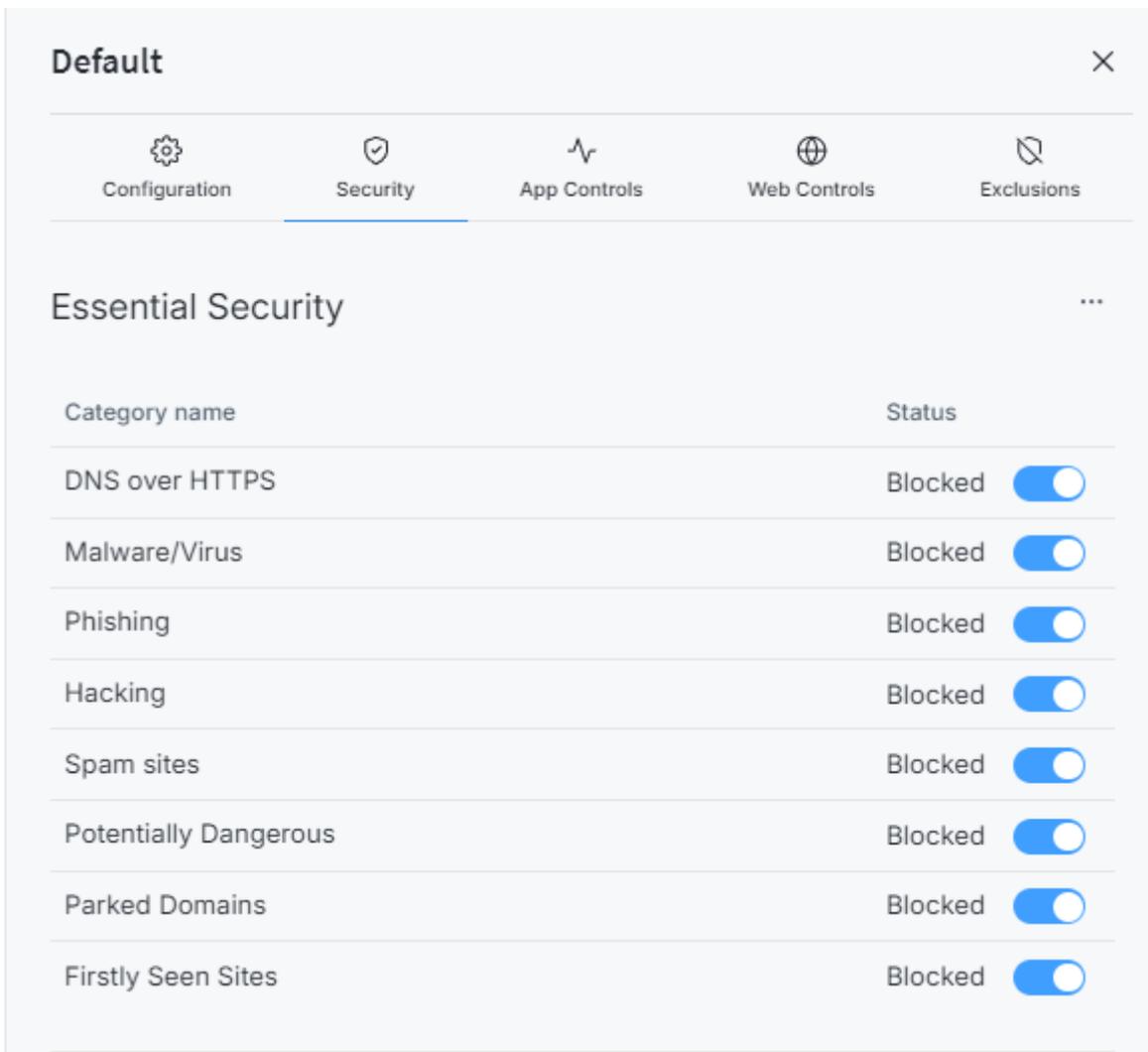
ZenArmor has a robust set of rules and policies you can enforce. The free version they offer will enforce "essential" security rules for up to 100 devices. You can find the policies and configure them by navigating to the Policies tab under the ZenArmor section of the sidebar in your OPNsense Web GUI:



This will bring you to your Policy page. The free version allows for 1 set of default policies.



To configure these policies, click on default. The free version of this will let you configure the following policies:



After testing out the free version, I opted to pay for the Home edition for \$9.99 a month. This unlocks additional configuration and reporting, along with daily updated rulesets. The security options unlocked are as follows:

Advanced Security



Category name	Status
Recent Malware/Phishing/Virus Outbreaks	Blocked <input checked="" type="checkbox"/>
Botnet C&C NEW	Blocked <input checked="" type="checkbox"/>
Botnet DGA Domains NEW	Blocked <input checked="" type="checkbox"/>
DNS Tunneling NEW	Allowed <input type="checkbox"/>
Compromised Website	Allowed <input type="checkbox"/>
Spyware and Adware	Blocked <input checked="" type="checkbox"/>
Keyloggers and Monitoring	Blocked <input checked="" type="checkbox"/>
Proxy	Allowed <input type="checkbox"/>
Dead Sites	Allowed <input type="checkbox"/>
Dynamic DNS Sites	Allowed <input type="checkbox"/>
Newly Registered Sites	Allowed <input type="checkbox"/>
Newly Recovered Sites	Allowed <input type="checkbox"/>
Malformed DNS Packet NEW	Blocked <input checked="" type="checkbox"/>

More information about these security rules can be found in ZenArmor's documentation under the [Managing Policies](#) section.

Revision #4

Created 17 March 2024 07:27:10 by Austin

Updated 17 March 2024 19:39:51 by Austin